National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 – 15 Aug 2024 Vol. 11 No. 15
https://nciipc.gov.in/

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 1password					
Product: 1password					
Affected Version(s): From (including) 8.0 Up to (excluding) 8.10.36					
N/A	06-Aug-2024	7.8	1Password 8 before 8.10.36 for macOS allows local attackers to exfiltrate vault items because XPC inter-process communication validation is insufficient. **CVE ID: CVE-2024-42219**	https://support.1password.com/kb/202408a/	A-1PA-1PAS-080824/1
Affected Version(s): From (including) 8.0 Up to (excluding) 8.10.38					
N/A	06-Aug-2024	4.7	1Password 8 before 8.10.38 for macOS allows local attackers to exfiltrate vault items by bypassing macOS-specific security mechanisms. **CVE ID: CVE-2024-42218**	https://support.1password.com/kb/202408/	A-1PA-1PAS-080824/2
Vendor: Adobe					
Product: acrobat					
Affected Version(s): From (including) 20.001.30005 Up to (excluding) 20.005.30655					
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/3

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39422**		
Out-of-bounds Write	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39423**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/4
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/5

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39424**		
Out-of-bounds Read	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39426**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/6

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41830**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/7
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41831**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/8

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could result in arbitrary code execution in the context of the current user. This issue occurs when the state of a resource changes between its check-time and use-time, allowing an attacker to manipulate the resource. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39420**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/9
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/10

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Condition vulnerability that could lead to privilege escalation. Exploitation of this issue require local low-privilege access to the affected system and attack complexity is high. **CVE ID: CVE-2024-39425**		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41832**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/11
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965,	https://helpx.adobe.com/security/products/ac	A-ADO-ACRO-080824/12

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			24.002.20964, 24.001.30123 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-2024-41833**	robat/apsb24-57.html	
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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/apsb24-57.html	A-ADO-ACRO-080824/13

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-41834**		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41835**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/14
Affected Version(s): From (including) 20.001.3005 Up to (excluding) 20.005.30655					
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39383**		
Affected Version(s): From (including) 24.001.20604 Up to (excluding) 24.001.30159					
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39383**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/16
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/17

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-2024-39422**		
Out-of-bounds Write	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39423**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/18
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/19

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

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-2024-39424**		
Out-of-bounds Read	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39426**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/20
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965,	https://helpx.adobe.com/security/products/ac	A-ADO-ACRO-080824/21

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			24.002.20964, 24.001.30123 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-2024-41830**	robat/apsb24-57.html	
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41831**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/22
Time-of-check Time-of-use (TOCTOU)	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964,	https://helpx.adobe.com/security/products/ac	A-ADO-ACRO-080824/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could result in arbitrary code execution in the context of the current user. This issue occurs when the state of a resource changes between its check-time and use-time, allowing an attacker to manipulate the resource. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39420**	robat/apsb24-57.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to privilege escalation.	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/24

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue require local low-privilege access to the affected system and attack complexity is high. **CVE ID: CVE-2024-39425**		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41832**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/25
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41833**		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41834**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/27

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41835**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/28
Product: acrobat_dc					
Affected Version(s): From (including) 15.008.20082 Up to (excluding) 24.002.21005					
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/29

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39422**		
Out-of-bounds Write	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39423**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/30
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/31

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39424**		
Out-of-bounds Read	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39426**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/32
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41830**		
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41831**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/34
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/35

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Condition vulnerability that could result in arbitrary code execution in the context of the current user. This issue occurs when the state of a resource changes between its check-time and use-time, allowing an attacker to manipulate the resource. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39420**		
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to privilege escalation. Exploitation of this issue require local low-privilege access to the affected system and	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/36

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack complexity is high. **CVE ID: CVE-2024-39425**		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41832**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/37
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/38

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41833**		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41834**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/39
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/40

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2024-41835**		
Affected Version(s): From (including) 24.002.20964 Up to (excluding) 24.002.21005					
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39383**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/41
Product: acrobat_reader					
Affected Version(s): From (including) 20.001.3005 Up to (excluding) 20.005.30655					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39383**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/42
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39422**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/43

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39423**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/44
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39424**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/45

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39426**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/46
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user.	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/47

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41830**		
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41831**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/48
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could result in arbitrary code execution in the	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/49

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. This issue occurs when the state of a resource changes between its check-time and use-time, allowing an attacker to manipulate the resource. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39420**		
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to privilege escalation. Exploitation of this issue require local low-privilege access to the affected system and attack complexity is high. **CVE ID: CVE-2024-39425**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/50

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41832**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/51
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41833**		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41834**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/53
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability that could lead to	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41835**		
Product: acrobat_reader_dc					
Affected Version(s): From (including) 15.008.20082 Up to (excluding) 24.002.21005					
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39422**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/55
Out-of-bounds Write	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964,	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/56

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			24.001.30123 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-2024-39423**		
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39424**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/57
Out-of-bounds Read	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964,	https://helpx.adobe.com/security/products/ac	A-ADO-ACRO-080824/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			24.001.30123 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39426**	robat/apsb24-57.html	
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/59

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41830		
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41831**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/60
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could result in arbitrary code execution in the context of the current user. This issue occurs when the state of a resource changes	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/61

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between its check-time and use-time, allowing an attacker to manipulate the resource. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39420**		
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to privilege escalation. Exploitation of this issue require local low-privilege access to the affected system and attack complexity is high. **CVE ID: CVE-2024-39425**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/62
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/63

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41832**		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/64

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41833		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41834**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/65
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41835**		
Affected Version(s): From (including) 24.002.20964 Up to (excluding) 24.002.21005					
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39383**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-080824/67
Product: bridge					
Affected Version(s): * Up to (excluding) 13.0.9					
Out-of-bounds Write	14-Aug-2024	7.8	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the	https://helpx.adobe.com/security/products/bridge/apsb24-59.html	A-ADO-BRID-080824/68

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39386**		
Out-of-bounds Write	14-Aug-2024	7.8	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41840**	https://helpx.adobe.com/security/products/bridge/apsb24-59.html	A-ADO-BRID-080824/69
Out-of-bounds Read	14-Aug-2024	5.5	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/bridge/apsb24-59.html	A-ADO-BRID-080824/70

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39387**		
Affected Version(s): From (including) 14.0.0 Up to (excluding) 14.1.2					
Out-of-bounds Write	14-Aug-2024	7.8	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39386**	https://helpx.adobe.com/security/products/bridge/apsb24-59.html	A-ADO-BRID-080824/71
Out-of-bounds Write	14-Aug-2024	7.8	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41840**	https://helpx.adobe.com/security/products/bridge/apsb24-59.html	A-ADO-BRID-080824/72

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Aug-2024	5.5	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39387**	https://helpx.adobe.com/security/products/bridge/apsb24-59.html	A-ADO-BRID-080824/73
Product: commerce					
Affected Version(s): * Up to (including) 2.4.3					
Unrestricted Upload of File with Dangerous Type	14-Aug-2024	9	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/74

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server. Exploitation of this issue does not require user interaction, but attack complexity is high and scope is changed. **CVE ID: CVE-2024-39397**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39401**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/75
Improper Neutralization of Special Elements used in an OS Command ('OS	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/76

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39402**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	8.1	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an admin attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link. Confidentiality and integrity impact is high as it affects other admin accounts. **CVE ID: CVE-2024-39400**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/77

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. A low-privileged attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39399**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/78
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/79

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary file system read. An attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	7.6	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality impact is high due to the attacker being able to	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/80

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exfiltrate sensitive information. **CVE ID: CVE-2024-39403**		
Improper Restriction of Excessive Authentication Attempts	14-Aug-2024	7.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to perform brute force attacks and potentially gain unauthorized access to accounts. Exploitation of this issue does not require user interaction, but attack complexity is high. **CVE ID: CVE-2024-39398**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/81
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/82

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39408**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/83

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39409		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	5.5	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39410**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/84
N/A	14-Aug-2024	5.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/85

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass security measures to view and edit low-sensitivity information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39418**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39404**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/86
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/87

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39405**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39407**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/88
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8,	https://helpx.adobe.com/security/products/m	A-ADO-COMM-080824/89

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39411**	agento/apsb24-61.html	
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/90

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39412		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39413**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/91
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39414**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39415**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/93
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/94

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39416**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39417**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/95
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/96

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39419**		
Affected Version(s): 2.4.4					
Unrestricted Upload of File with Dangerous Type	14-Aug-2024	9	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue does not require user interaction, but attack complexity is	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			high and scope is changed. **CVE ID: CVE-2024-39397**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39401**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/98
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/99

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39402**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	8.1	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an admin attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link. Confidentiality and integrity impact is high as it affects other admin accounts. **CVE ID: CVE-2024-39400**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/100
Improper Limitation of a Pathname to a Restricted	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/101

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. A low-privileged attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39399**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to gain access to files	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/102

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	7.6	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality impact is high due to the attacker being able to exfiltrate sensitive information. **CVE ID: CVE-2024-39403**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/103

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	14-Aug-2024	7.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to perform brute force attacks and potentially gain unauthorized access to accounts. Exploitation of this issue does not require user interaction, but attack complexity is high. **CVE ID: CVE-2024-39398**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/104
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/105

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39408**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39409**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/106
Cross-Site Request	14-Aug-2024	5.5	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8,	https://helpx.adobe.com/security/products/m	A-ADO-COMM-080824/107

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39410**	agento/apsb24-61.html	
N/A	14-Aug-2024	5.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures to view and edit low-sensitivity information.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39418**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39404**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/109
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/110

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39405**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39407**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/111
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39411**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39412**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/113
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8,	https://helpx.adobe.com/security/products/m	A-ADO-COMM-080824/114

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39413**	agento/apsb24-61.html	
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/115

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39414		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39415**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/116
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39416**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39417**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/118
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/119

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39419**		
Affected Version(s): 2.4.5					
Unrestricted Upload of File with Dangerous Type	14-Aug-2024	9	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue does not require user interaction, but attack complexity is high and scope is changed. **CVE ID: CVE-2024-39397**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/120

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39401**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/121
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction and scope is changed. **CVE ID: CVE-2024-39402**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	8.1	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an admin attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link. Confidentiality and integrity impact is high as it affects other admin accounts. **CVE ID: CVE-2024-39400**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/123
Improper Limitation of a Pathname to a Restricted Directory	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/124

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. A low-privileged attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39399**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/125

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	7.6	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality impact is high due to the attacker being able to exfiltrate sensitive information. **CVE ID: CVE-2024-39403**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/126
Improper Restriction of Excessive Authentica	14-Aug-2024	7.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an	https://helpx.adobe.com/security/products/m	A-ADO-COMM-080824/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			Improper Restriction of Excessive Authentication Attempts vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to perform brute force attacks and potentially gain unauthorized access to accounts. Exploitation of this issue does not require user interaction, but attack complexity is high. **CVE ID: CVE-2024-39398**	agento/apsb24-61.html	
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39408**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39409**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/129
Cross-Site Request Forgery (CSRF)	14-Aug-2024	5.5	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/130

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39410**		
N/A	14-Aug-2024	5.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures to view and edit low-sensitivity information. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/131

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39418		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39404**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/132
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/133

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39405**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39407**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/134
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/135

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39411**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39412**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/136
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/137

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39413**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39414**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/138

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39415**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/139
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/140

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not require user interaction. **CVE ID: CVE-2024-39416**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39417**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/141
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/142

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39419**		
Affected Version(s): 2.4.6					
Unrestricted Upload of File with Dangerous Type	14-Aug-2024	9	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue does not require user interaction, but attack complexity is high and scope is changed. **CVE ID: CVE-2024-39397**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/143
Improper Neutralizat	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1,	https://helpx.adobe.com/secur	A-ADO-COMM-080824/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39401**	ity/products/magento/apsb24-61.html	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/145

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39402		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	8.1	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an admin attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link. Confidentiality and integrity impact is high as it affects other admin accounts. **CVE ID: CVE-2024-39400**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/146
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/147

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could lead to arbitrary file system read. A low-privileged attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39399**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	7.6	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality impact is high due to the attacker being able to exfiltrate sensitive information. **CVE ID: CVE-2024-39403**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/149
Improper Restriction of Excessive Authentica	14-Aug-2024	7.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Restriction of	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			Excessive Authentication Attempts vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to perform brute force attacks and potentially gain unauthorized access to accounts. Exploitation of this issue does not require user interaction, but attack complexity is high. **CVE ID: CVE-2024-39398**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39408**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39409**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/152
Cross-Site Request Forgery (CSRF)	14-Aug-2024	5.5	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39410**		
N/A	14-Aug-2024	5.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures to view and edit low-sensitivity information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39418**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/154

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39404**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/155
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/156

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not require user interaction. **CVE ID: CVE-2024-39405**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39407**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/157
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/158

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39411**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39412**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/159
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/160

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39413**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39414**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/161
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier	https://helpx.adobe.com/security/products/m	A-ADO-COMM-080824/162

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39415**	agento/apsb24-61.html	
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/163

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39416		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39417**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/164
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39419**		
Affected Version(s): 2.4.7					
Unrestricted Upload of File with Dangerous Type	14-Aug-2024	9	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue does not require user interaction, but attack complexity is high and scope is changed. **CVE ID: CVE-2024-39397**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/166
Improper Neutralization of Special Elements	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39401**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39402**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/168

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	8.1	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an admin attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link. Confidentiality and integrity impact is high as it affects other admin accounts. **CVE ID: CVE-2024-39400**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/169
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary file system read. A low-privileged attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39399**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction and scope is changed. **CVE ID: CVE-2024-39406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	7.6	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality impact is high due to the attacker being able to exfiltrate sensitive information. **CVE ID: CVE-2024-39403**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/172
Improper Restriction of Excessive Authentication Attempts	14-Aug-2024	7.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Restriction of Excessive Authentication	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/173

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Attempts vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to perform brute force attacks and potentially gain unauthorized access to accounts. Exploitation of this issue does not require user interaction, but attack complexity is high. **CVE ID: CVE-2024-39398**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/174

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction. **CVE ID: CVE-2024-39408**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39409**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/175
Cross-Site Request Forgery (CSRF)	14-Aug-2024	5.5	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39410**		
N/A	14-Aug-2024	5.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures to view and edit low-sensitivity information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39418**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/177
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8,	https://helpx.adobe.com/security/products/m	A-ADO-COMM-080824/178

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39404**	agento/apsb24-61.html	
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/179

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39405		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39407**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/180
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39411**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39412**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/182
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/183

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39413**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39414**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/184
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/185

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39415**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39416**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/186

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39417**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/187
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-COMM-080824/188

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not require user interaction. **CVE ID: CVE-2024-39419**		
Product: dimension					
Affected Version(s): * Up to (including) 3.4.11					
Use After Free	14-Aug-2024	7.8	Dimension versions 3.4.11 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-2024-20789**	https://helpx.adobe.com/security/products/dimension/apsb24-47.html	A-ADO-DIME-080824/189
Out-of-bounds Write	14-Aug-2024	7.8	Dimension versions 3.4.11 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/dimension/apsb24-47.html	A-ADO-DIME-080824/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-34124		
Untrusted Search Path	14-Aug-2024	7.8	Dimension versions 3.4.11 and earlier are affected by an Untrusted Search Path vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by inserting a malicious file into the search path, which the application might execute instead of the legitimate file. This could occur if the application uses a search path to locate executables or libraries. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-41865**	https://helpx.adobe.com/security/products/dimension/apsb24-47.html	A-ADO-DIME-080824/191
Out-of-bounds Read	14-Aug-2024	5.5	Dimension versions 3.4.11 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx.adobe.com/security/products/dimension/apsb24-47.html	A-ADO-DIME-080824/192

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-20790**		
Out-of-bounds Read	14-Aug-2024	5.5	Dimension versions 3.4.11 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-2024-34125**	https://helpx.adobe.com/security/products/dimension/apsb24-47.html	A-ADO-DIME-080824/193
Out-of-bounds Read	14-Aug-2024	5.5	Dimension versions 3.4.11 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	https://helpx.adobe.com/security/products/dimension/apsb24-47.html	A-ADO-DIME-080824/194

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34126**		
Product: illustrator					
Affected Version(s): From (including) 27.0 Up to (excluding) 27.9.5					
N/A	14-Aug-2024	7.8	Illustrator versions 28.5, 27.9.4 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-2024-41856**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/195
Affected Version(s): From (including) 27.0.0 Up to (excluding) 27.9.5					
Out-of-bounds Write	14-Aug-2024	7.8	Illustrator versions 28.5, 27.9.4 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/illustrator/apsb24-45.html	A-ADO-ILLU-080824/196

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

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-2024-34133**		
N/A	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by an Improper Input Validation vulnerability that could lead to an application denial-of-service condition. An attacker could exploit this vulnerability to render the application unresponsive or terminate its execution. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34118**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/197
Out-of-bounds Read	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 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	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/198

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34134**		
Out-of-bounds Read	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 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-2024-34135**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/199
NULL Pointer Dereference	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/200

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34136**		
NULL Pointer Dereference	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS) condition. An attacker could exploit this vulnerability to crash the application, resulting in a DoS. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34137**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/201
NULL Pointer Dereference	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/202

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34138**		
Affected Version(s): From (including) 28.0 Up to (excluding) 28.6					
Out-of-bounds Write	14-Aug-2024	7.8	Illustrator versions 28.5, 27.9.4 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-2024-34133**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/203
N/A	14-Aug-2024	7.8	Illustrator versions 28.5, 27.9.4 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/204

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-2024-41856**		
N/A	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by an Improper Input Validation vulnerability that could lead to an application denial-of-service condition. An attacker could exploit this vulnerability to render the application unresponsive or terminate its execution. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34118**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/205
Out-of-bounds Read	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/206

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

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-2024-34134**		
Out-of-bounds Read	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 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-2024-34135**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/207
NULL Pointer Dereference	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/208

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34136**		
NULL Pointer Dereference	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS) condition. An attacker could exploit this vulnerability to crash the application, resulting in a DoS. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34137**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	A-ADO-ILLU-080824/209
NULL Pointer Dereference	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference	https://helpx.adobe.com/security/products/ill	A-ADO-ILLU-080824/210

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34138**	ustrator/apsb24-45.html	
Product: indesign					
Affected Version(s): * Up to (excluding) 18.5.3					
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-39389**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-39390**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/212
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-39391**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/213
Out-of-bounds Read	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/214

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39393**		
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-39394**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/215
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/216

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41850**		
Integer Overflow or Wraparound	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41851**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/217
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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.	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/218

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41852**		
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41853**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/219
Out-of-bounds Read	14-Aug-2024	7.1	InDesign Desktop versions ID19.4, ID18.5.2 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/indesign/apsb24-56.html	A-ADO-INDE-080824/220

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-34127**		
NULL Pointer Dereference	14-Aug-2024	5.5	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a DoS condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39395**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/221
Out-of-bounds Read	14-Aug-2024	5.5	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/222

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-2024-41854**		
NULL Pointer Dereference	14-Aug-2024	5.5	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41866**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/223
Affected Version(s): From (including) 19.0 Up to (excluding) 19.5					
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39389**		
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-39390**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/225
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-39391**		
Out-of-bounds Read	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39393**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/227
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/228

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-39394**		
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41850**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/229
Integer Overflow or Wraparound	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41851**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/230

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41852**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/231
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41853**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/232
Out-of-bounds Read	14-Aug-2024	7.1	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read	https://helpx.adobe.com/security/products/in	A-ADO-INDE-080824/233

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34127**	design/apsb24-56.html	
NULL Pointer Dereference	14-Aug-2024	5.5	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a DoS condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39395**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/234

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Aug-2024	5.5	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41854**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/235
NULL Pointer Dereference	14-Aug-2024	5.5	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	A-ADO-INDE-080824/236

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-41866**		
Product: magento					
Affected Version(s): * Up to (including) 2.4.3					
Unrestricted Upload of File with Dangerous Type	14-Aug-2024	9	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue does not require user interaction, but attack complexity is high and scope is changed. **CVE ID: CVE-2024-39397**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/237
Improper Neutralization of Special Elements used in an OS	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39401**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39402**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/239
Improper Neutralization of Input During	14-Aug-2024	8.1	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier	https://helpx.adobe.com/security/products/m	A-ADO-MAGE-080824/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an admin attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link. Confidentiality and integrity impact is high as it affects other admin accounts. **CVE ID: CVE-2024-39400**	agento/apsb24-61.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. A low-privileged attacker could exploit this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/241

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39399**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39406**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/242

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	7.6	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality impact is high due to the attacker being able to exfiltrate sensitive information. **CVE ID: CVE-2024-39403**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/243
Improper Restriction of Excessive Authentication Attempts	14-Aug-2024	7.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability that could result in a security feature	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/244

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass. An attacker could exploit this vulnerability to perform brute force attacks and potentially gain unauthorized access to accounts. Exploitation of this issue does not require user interaction, but attack complexity is high. **CVE ID: CVE-2024-39398**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39408**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/245

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39409**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/246
Cross-Site Request Forgery (CSRF)	14-Aug-2024	5.5	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39410**		
N/A	14-Aug-2024	5.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures to view and edit low-sensitivity information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39418**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/248
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/249

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39404**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39405**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39407**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/251
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not require user interaction. **CVE ID: CVE-2024-39411**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39412**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/253
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39413**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39414**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/255
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/256

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39415**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39416**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/257
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier	https://helpx.adobe.com/security/products/m	A-ADO-MAGE-080824/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39417**	agento/apsb24-61.html	
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/259

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39419		
Affected Version(s): 2.4.4					
Unrestricted Upload of File with Dangerous Type	14-Aug-2024	9	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue does not require user interaction, but attack complexity is high and scope is changed. **CVE ID: CVE-2024-39397**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/260
Improper Neutralization of Special Elements used in an OS Command ('OS	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/261

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39401**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39402**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/262
Improper Neutralization of Input During Web Page Generation	14-Aug-2024	8.1	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/263

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability could allow an admin attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link. Confidentiality and integrity impact is high as it affects other admin accounts. **CVE ID: CVE-2024-39400**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. A low-privileged attacker could exploit this vulnerability to gain access to files and directories that are outside the	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/264

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39399**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39406**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/265
Improper Neutralization of Input During	14-Aug-2024	7.6	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier	https://helpx.adobe.com/security/products/m	A-ADO-MAGE-080824/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality impact is high due to the attacker being able to exfiltrate sensitive information. **CVE ID: CVE-2024-39403**	agento/apsb24-61.html	
Improper Restriction of Excessive Authentication Attempts	14-Aug-2024	7.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to perform brute force	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/267

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks and potentially gain unauthorized access to accounts. Exploitation of this issue does not require user interaction, but attack complexity is high. **CVE ID: CVE-2024-39398**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39408**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/268
Cross-Site Request	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier	https://helpx.adobe.com/security/products/m	A-ADO-MAGE-080824/269

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39409**	agento/apsb24-61.html	
Cross-Site Request Forgery (CSRF)	14-Aug-2024	5.5	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/270

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39410**		
N/A	14-Aug-2024	5.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures to view and edit low-sensitivity information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39418**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/271
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39404**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39405**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/273
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/274

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39407**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39411**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/275

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39412**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/276
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/277

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not require user interaction. **CVE ID: CVE-2024-39413**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39414**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/278
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39415**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39416**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/280
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/281

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39417**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39419**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/282
Affected Version(s): 2.4.5					
Unrestricted Upload of	14-Aug-2024	9	Adobe Commerce versions 2.4.7-p1,	https://helpx.adobe.com/secur	A-ADO-MAGE-080824/283

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue does not require user interaction, but attack complexity is high and scope is changed. **CVE ID: CVE-2024-39397**	ity/products/magento/apsb24-61.html	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39401**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39402**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/285
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	8.1	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an admin attacker to inject and execute arbitrary JavaScript	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link. Confidentiality and integrity impact is high as it affects other admin accounts. **CVE ID: CVE-2024-39400**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. A low-privileged attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction and scope is changed. **CVE ID: CVE-2024-39399**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39406**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/288
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	7.6	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/289

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality impact is high due to the attacker being able to exfiltrate sensitive information. **CVE ID: CVE-2024-39403**		
Improper Restriction of Excessive Authentication Attempts	14-Aug-2024	7.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to perform brute force attacks and potentially gain unauthorized access to accounts. Exploitation of this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not require user interaction, but attack complexity is high. **CVE ID: CVE-2024-39398**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39408**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/291
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/292

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39409**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	5.5	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/293

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39410		
N/A	14-Aug-2024	5.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures to view and edit low-sensitivity information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39418**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/294
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/295

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39404**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39405**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/296
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39407**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39411**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/298
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/299

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39412**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39413**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/300

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39414**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/301
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not require user interaction. **CVE ID: CVE-2024-39415**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39416**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/303
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39417**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39419**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/305
Affected Version(s): 2.4.6					
Unrestricted Upload of File with Dangerous Type	14-Aug-2024	9	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue does not require user interaction, but attack complexity is high and scope is changed. **CVE ID: CVE-2024-39397**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/307

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39401		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39402**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/308
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	8.1	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an admin attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction, such as convincing a victim to click on a malicious link. Confidentiality and integrity impact is high as it affects other admin accounts. **CVE ID: CVE-2024-39400**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. A low-privileged attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39399**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/310

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39406**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/311
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	7.6	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality impact is high due to the attacker being able to exfiltrate sensitive information. **CVE ID: CVE-2024-39403**		
Improper Restriction of Excessive Authentication Attempts	14-Aug-2024	7.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to perform brute force attacks and potentially gain unauthorized access to accounts. Exploitation of this issue does not require user interaction, but	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack complexity is high. **CVE ID: CVE-2024-39398**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39408**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/314
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39409**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	5.5	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39410**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/316

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	5.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures to view and edit low-sensitivity information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39418**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/317
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/318

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39404**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39405**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/319
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/320

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39407**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39411**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/321
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/322

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39412**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39413**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/323
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8,	https://helpx.adobe.com/security/products/m	A-ADO-MAGE-080824/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39414**	agento/apsb24-61.html	
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/325

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39415		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39416**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/326
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39417**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39419**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/328
Affected Version(s): 2.4.7					
Unrestricted Upload of File with Dangerous Type	14-Aug-2024	9	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue does not require user interaction, but attack complexity is high and scope is changed. **CVE ID: CVE-2024-39397**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39401**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/330

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Aug-2024	8.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-39402**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/331
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	8.1	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an admin attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			convincing a victim to click on a malicious link. Confidentiality and integrity impact is high as it affects other admin accounts. **CVE ID: CVE-2024-39400**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. A low-privileged attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39399**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/333
Improper Limitation of a	14-Aug-2024	7.7	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8,	https://helpx.adobe.com/security/products/m	A-ADO-MAGE-080824/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-39406**	agento/apsb24-61.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	7.6	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality impact is high due to the attacker being able to exfiltrate sensitive information. **CVE ID: CVE-2024-39403**		
Improper Restriction of Excessive Authentication Attempts	14-Aug-2024	7.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to perform brute force attacks and potentially gain unauthorized access to accounts. Exploitation of this issue does not require user interaction, but attack complexity is high. **CVE ID: CVE-2024-39398**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/336

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39408**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/337
Cross-Site Request Forgery (CSRF)	14-Aug-2024	6.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39409**		
Cross-Site Request Forgery (CSRF)	14-Aug-2024	5.5	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-39410**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/339
N/A	14-Aug-2024	5.4	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an	https://helpx.adobe.com/security/products/m	A-ADO-MAGE-080824/340

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures to view and edit low-sensitivity information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39418**	agento/apsb24-61.html	
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/341

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39404		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39405**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/342
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39407**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39411**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/344
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/345

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39412**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39413**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/346
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/347

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39414**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39415**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39416**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/349
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/350

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not require user interaction. **CVE ID: CVE-2024-39417**		
N/A	14-Aug-2024	4.3	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-39419**	https://helpx.adobe.com/security/products/magento/apsb24-61.html	A-ADO-MAGE-080824/351
Product: photoshop					
Affected Version(s): From (including) 24.2 Up to (excluding) 24.7.4					
Use After Free	14-Aug-2024	7.8	Photoshop Desktop versions 24.7.3, 25.9.1 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user.	https://helpx.adobe.com/security/products/photoshop/apsb24-49.html	A-ADO-PHOT-080824/352

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34117**		
Affected Version(s): From (including) 25.0 Up to (excluding) 25.11					
Use After Free	14-Aug-2024	7.8	Photoshop Desktop versions 24.7.3, 25.9.1 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34117**	https://helpx.adobe.com/security/products/photoshop/apsb24-49.html	A-ADO-PHOT-080824/353
Product: substance_3d_designer					
Affected Version(s): * Up to (excluding) 14.0					
Out-of-bounds Write	14-Aug-2024	7.8	Substance3D - Designer versions 13.1.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/substance3d_designer/apsb24-67.html	A-ADO-SUBS-080824/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-41864**		
Product: substance_3d_sampler					
Affected Version(s): * Up to (excluding) 4.5.1					
Out-of-bounds Read	14-Aug-2024	5.5	Substance3D - Sampler versions 4.5 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-2024-41860**	https://helpx.adobe.com/security/products/substance3d-sampler/apsb24-65.html	A-ADO-SUBS-080824/355
Out-of-bounds Read	14-Aug-2024	5.5	Substance3D - Sampler versions 4.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this	https://helpx.adobe.com/security/products/substance3d-sampler/apsb24-65.html	A-ADO-SUBS-080824/356

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-2024-41861**		
Out-of-bounds Read	14-Aug-2024	5.5	Substance3D - Sampler versions 4.5 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-2024-41862**	https://helpx.adobe.com/security/products/substance3d-sampler/apsb24-65.html	A-ADO-SUBS-080824/357
Out-of-bounds Read	14-Aug-2024	5.5	Substance3D - Sampler versions 4.5 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/substance3d-sampler/apsb24-65.html	A-ADO-SUBS-080824/358

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41863**		
Product: substance_3d_stager					
Affected Version(s): * Up to (excluding) 3.0.3					
Use After Free	14-Aug-2024	7.8	Substance3D - Stager versions 3.0.2 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-2024-39388**	N/A	A-ADO-SUBS-080824/359
Vendor: adrianmercurio					
Product: vehicle_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Aug-2024	9.8	A vulnerability was found in itsourcecode Vehicle Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file mybill.php. The manipulation of the	N/A	A-ADR-VEHI-080824/360

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7794**		
Vendor: angeljudesuarez					
Product: airline_reservation_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	9.8	A vulnerability was found in itsourcecode Airline Reservation System 1.0. It has been classified as critical. Affected is the function login/login2 of the file /admin/login.php of the component Admin Login Page. The manipulation of the argument username 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-273624. **CVE ID: CVE-2024-7498**	N/A	A-ANG-AIRL-080824/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	9.8	A vulnerability was found in itsourcecode Airline Reservation System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file flights.php. The manipulation of the argument departure_airport_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273625 was assigned to this vulnerability. **CVE ID: CVE-2024-7499**	N/A	A-ANG-AIRL-080824/362
N/A	06-Aug-2024	8.8	A vulnerability has been found in itsourcecode Airline Reservation System 1.0 and classified as critical. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument page leads to file inclusion. The attack can be	N/A	A-ANG-AIRL-080824/363

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273622 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-7496**		
N/A	06-Aug-2024	8.8	A vulnerability was found in itsourcecode Airline Reservation System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/index.php. The manipulation of the argument page leads to file inclusion. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273623. **CVE ID: CVE-2024-7497**	N/A	A-ANG-AIRL-080824/364
Product: billing_system					
Affected Version(s): 1.0					
Improper Neutralizat	15-Aug-2024	9.8	A vulnerability classified as critical	N/A	A-ANG-BILL-080824/365

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			has been found in itsourcecode Billing System 1.0. This affects an unknown part of the file addbill.php. The manipulation of the argument owners_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7839**		
Product: placement_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in itsourcecode Placement Management System 1.0. Affected is an unknown function of the file login.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier	N/A	A-ANG-PLAC-080824/366

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability is VDB-273540. **CVE ID: CVE-2024-7449**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-2024	9.8	A vulnerability was found in itsourcecode Placement Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file apply_now.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-273542 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-7451**	N/A	A-ANG-PLAC-080824/367
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-2024	9.8	A vulnerability was found in itsourcecode Placement Management System 1.0. It has been classified as critical. This affects an unknown part of the file view_company.php	N/A	A-ANG-PLAC-080824/368

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273543. **CVE ID: CVE-2024-7452**		
Unrestricted Upload of File with Dangerous Type	04-Aug-2024	8.8	A vulnerability has been found in itsourcecode Placement Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /resume_upload.php of the component Image Handler. The manipulation of the argument fileToUpload leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier	N/A	A-ANG-PLAC-080824/369

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-273541 was assigned to this vulnerability. **CVE ID: CVE-2024-7450**		
Product: tailoring_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	9.8	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been classified as critical. This affects an unknown part of the file /incedit.php?id=4. The manipulation of the argument id/inccat/desc/date/amount leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7680**	N/A	A-ANG-TAIL-080824/370
Vendor: Apache					
Product: cloudstack					
Affected Version(s): From (including) 4.10.0.0 Up to (excluding) 4.18.2.3					
Incorrect Authorization	07-Aug-2024	7.2	CloudStack account-users by default use username and password based authentication for	https://cloudstack.apache.org/blog/security-release-advisory-	A-APA-CLOU-080824/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			API and UI access. Account-users can generate and register randomised API and secret keys and use them for the purpose of API-based automation and integrations. Due to an access permission validation issue that affects Apache CloudStack versions 4.10.0 up to 4.19.1.0, domain admin accounts were found to be able to query all registered account-users API and secret keys in an environment, including that of a root admin. An attacker who has domain admin access can exploit this to gain root admin and other-account privileges and perform malicious operations that can result in compromise of resources integrity and confidentiality, data loss, denial of service and availability of CloudStack	4.19.1.1-4.18.2.3	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			managed infrastructure. Users are recommended to upgrade to Apache CloudStack 4.18.2.3 or 4.19.1.1, or later, which addresses this issue. Additionally, all account-user API and secret keys should be regenerated. **CVE ID: CVE-2024-42062**		
Affected Version(s): From (including) 4.19.0.0 Up to (excluding) 4.19.1.1					
Incorrect Authorization	07-Aug-2024	7.2	CloudStack account-users by default use username and password based authentication for API and UI access. Account-users can generate and register randomised API and secret keys and use them for the purpose of API-based automation and integrations. Due to an access permission validation issue that affects Apache CloudStack versions 4.10.0 up to 4.19.1.0, domain	https://cloudstack.apache.org/blog/security-release-advisory-4.19.1.1-4.18.2.3	A-APA-CLOU-080824/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin accounts were found to be able to query all registered account-users API and secret keys in an environment, including that of a root admin. An attacker who has domain admin access can exploit this to gain root admin and other-account privileges and perform malicious operations that can result in compromise of resources integrity and confidentiality, data loss, denial of service and availability of CloudStack managed infrastructure. Users are recommended to upgrade to Apache CloudStack 4.18.2.3 or 4.19.1.1, or later, which addresses this issue. Additionally, all account-user API and secret keys should be regenerated. **CVE ID: CVE-2024-42062**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: linkis					
Affected Version(s): From (including) 1.3.2 Up to (excluding) 1.6.0					
Files or Directories Accessible to External Parties	02-Aug-2024	4.9	In Apache Linkis <= 1.5.0, Arbitrary file deletion in Basic management services on A user with an administrator account could delete any file accessible by the Linkis system user . Users are recommended to upgrade to version 1.6.0, which fixes this issue. **CVE ID: CVE-2024-27182**	https://lists.apache.org/thread/2of1p433h8rbq2bx525rtftnk19oz38h	A-APA-LINK-080824/373
Vendor: appleboy					
Product: gorush					
Affected Version(s): * Up to (including) 1.18.4					
Use of a Broken or Risky Cryptographic Algorithm	06-Aug-2024	9.1	An issue discovered in the RunHTTPServer function in Gorush v1.18.4 allows attackers to intercept and manipulate data due to use of deprecated TLS version.	N/A	A-APP-GORU-080824/374

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41270		
Vendor: automationanywhere					
Product: automation_360					
Affected Version(s): 21094					
Improper Neutralization of Formula Elements in a CSV File	06-Aug-2024	7.8	A CSV injection vulnerability in Automation Anywhere Automation 360 version 21094 allows attackers to execute arbitrary code via a crafted payload. **CVE ID: CVE-2024-41226**	N/A	A-AUT-AUTO-080824/375
Vendor: Baidu					
Product: ueditor					
Affected Version(s): * Up to (including) 1.4.3.3					
Unrestricted Upload of File with Dangerous Type	01-Aug-2024	6.1	A vulnerability was found in Baidu UEditor 1.4.3.3. It has been classified as problematic. This affects an unknown part of the file /ueditor/php/controller.php?action=uploadfile&encode=utf-8. The manipulation of the argument upfile leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been	N/A	A-BAI-UEDI-080824/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. The identifier VDB-273273 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7342**		
Affected Version(s): 1.4.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2024	6.1	A vulnerability was found in Baidu UEditor 1.4.2. It has been declared as problematic. This vulnerability affects unknown code of the file /ueditor142/php/controller.php?action=catchimage. The manipulation of the argument source[] leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273274 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this	N/A	A-BAI-UEDI-080824/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure but did not respond in any way. **CVE ID: CVE-2024-7343**		
Vendor: biscuitsec					
Product: biscuit-auth					
Affected Version(s): * Up to (excluding) 5.0.0					
N/A	01-Aug-2024	6.4	biscuit-rust is the Rust implementation of Biscuit, an authentication and authorization token for microservices architectures. Third-party blocks can be generated without transferring the whole token to the third-party authority. Instead, a ThirdPartyBlock request can be sent, providing only the necessary info to generate a third-party block and to sign it, which includes the public key of the previous block (used in the signature) and the public keys part of the token symbol table (for public key interning in datalog expressions). A third-part block	N/A	A-BIS-BISC-080824/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forged by a malicious user can trick the third-party authority into generating datalog trusting the wrong keypair. **CVE ID: CVE-2024-41949**		
Product: biscuit-java					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 4.0.0					
N/A	01-Aug-2024	5	biscuit-java is the java implementation of Biscuit, an authentication and authorization token for microservices architectures. Third-party blocks can be generated without transferring the whole token to the third-party authority. Instead, a ThirdPartyBlock request can be sent, providing only the necessary info to generate a third-party block and to sign it, which includes the public key of the previous block (used in the signature) and the public keys part of the token symbol table (for public key interning in datalog	N/A	A-BIS-BISC-080824/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			expressions). A third-part block request forged by a malicious user can trick the third-party authority into generating datalog trusting the wrong keypair. This vulnerability is fixed in 4.0.0. **CVE ID: CVE-2024-41948**		
Vendor: Calibre-ebook					
Product: calibre					
Affected Version(s): * Up to (including) 7.14.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	7.5	Path traversal in Calibre <= 7.14.0 allow unauthenticated attackers to achieve arbitrary file read. **CVE ID: CVE-2024-6781**	https://github.com/kovidgoyal/calibre/commit/bcd0ab12c41a887f8290a9b56e46c3a29038d9c4	A-CAL-CALI-080824/380
Affected Version(s): * Up to (including) 7.15.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.1	Unsanitized user-input in Calibre <= 7.15.0 allow users with permissions to perform full-text searches to achieve SQL injection on the SQLite database. **CVE ID: CVE-2024-7009**	https://github.com/kovidgoyal/calibre/commit/d56574285e8859d3d715eb7829784ee74337b7d7	A-CAL-CALI-080824/381
Improper Neutralization of Input During Web Page	06-Aug-2024	6.1	Unsanitized user-input in Calibre <= 7.15.0 allow attackers to	https://github.com/kovidgoyal/calibre/commit/863abac24e7bc3e5ca0b3307	A-CAL-CALI-080824/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			perform reflected cross-site scripting. **CVE ID: CVE-2024-7008**	362ff1953ba53fe0	
Vendor: casbin					
Product: casdoor					
Affected Version(s): 1.636.0					
Improper Certificate Validation	01-Aug-2024	7.5	An issue discovered in casdoor v1.636.0 allows attackers to obtain sensitive information via the ssh.InsecureIgnoreHostKey() method. **CVE ID: CVE-2024-41264**	N/A	A-CAS-CASD-080824/383
Vendor: celsiusbenelux					
Product: comfortkey					
Affected Version(s): * Up to (excluding) 24.1.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	7.5	A Local File Inclusion vulnerability has been found in ComfortKey, a product of Celsius Benelux. Using this vulnerability, an unauthenticated attacker may retrieve sensitive information about the underlying system. The vulnerability has been remediated in version 24.1.2. **CVE ID: CVE-2024-27120**	N/A	A-CEL-COMF-080824/384
Vendor: changingtec					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: hwatai_servisign					
Affected Version(s): * Up to (excluding) 1.0.24.0219					
Out-of-bounds Write	02-Aug-2024	4.3	The specific API in HWATAIServiSign Windows Version from CHANGING Information Technology does not properly validate the length of server-side inputs. When a user visits a spoofed website, unauthenticated remote attackers can cause a stack-based buffer overflow in the HWATAIServiSign, temporarily disrupting its service. **CVE ID: CVE-2024-40723**	N/A	A-CHA-HWAT-080824/385
Product: tcb_servisign					
Affected Version(s): * Up to (excluding) 1.0.24.0318					
N/A	02-Aug-2024	8.8	The specific API in TCBServiSign Windows Version from CHANGING Information Technology does not properly validate server-side input. When a user visits a spoofed website, unauthenticated remote attackers can modify the `HKEY_CURRENT_	N/A	A-CHA-TCB_-080824/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			USER` registry to execute arbitrary commands. **CVE ID: CVE-2024-40720**		
N/A	02-Aug-2024	8.8	The specific API in TCBServiSign Windows Version from CHANGING Information Technology does not properly validate server-side input. When a user visits a spoofed website, unauthenticated remote attackers can cause the TCBServiSign to load a DLL from an arbitrary path. **CVE ID: CVE-2024-40721**	N/A	A-CHA-TCB_-080824/387
Inadequate Encryption Strength	02-Aug-2024	6.5	The encryption strength of the authorization keys in CHANGING Information Technology TCBServiSign Windows Version is insufficient. When a remote attacker tricks a victim into visiting a malicious website, TCBServiSign will treat that website as a legitimate server and interact with it.	N/A	A-CHA-TCB_-080824/388

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-40719		
Out-of-bounds Write	02-Aug-2024	4.3	The specific API in TCBServiSign Windows Version from CHANGING Information Technology does does not properly validate the length of server-side input. When a user visits a spoofed website, unauthenticated remote attackers can cause a stack-based buffer overflow in the TCBServiSign, temporarily disrupting its service. **CVE ID: CVE-2024-40722**	N/A	A-CHA-TCB_-080824/389
Vendor: clastix					
Product: kamaji					
Affected Version(s): * Up to (excluding) edge-24.8.2					
N/A	12-Aug-2024	9.9	Kamaji is the Hosted Control Plane Manager for Kubernetes. In versions 1.0.0 and earlier, Kamaji uses an "open at the top" range definition in RBAC for etcd roles leading to some TCPs API servers being able to read, write, and delete the data of other	https://github.com/clastix/kamaji/commit/1731e8c2ed5148b125ecfbdf091ee177bd44f3db, https://github.com/clastix/kamaji/security/advisories/GHSA-6r4j-4rjc-8vw5	A-CLA-KAMA-080824/390

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control planes. This vulnerability is fixed in edge-24.8.2. **CVE ID: CVE-2024-42480**		
Vendor: code-projects					
Product: simple_ticket_booking					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	9.8	A vulnerability was found in code-projects Simple Ticket Booking 1.0. It has been classified as critical. Affected is an unknown function of the file register_insert.php of the component Registration Handler. The manipulation of the argument name/email/dob/password/Gender/phone leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7635**	N/A	A-COD-SIMP-080824/391
Improper Neutralization of Special Elements	12-Aug-2024	9.8	A vulnerability was found in code-projects Simple Ticket Booking 1.0. It has been	N/A	A-COD-SIMP-080824/392

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			declared as critical. Affected by this vulnerability is an unknown functionality of the file authenticate.php of the component Login. The manipulation of the argument email/password leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7636**		
Vendor: college_management_system_project					
Product: college_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	9.8	A vulnerability was found in code-projects College Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php of the component Login Page. The manipulation of the argument email/password leads to sql	N/A	A-COL-COLL-080824/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7681**		
Vendor: cysoft168					
Product: super_easy_enterprise_management_system					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Aug-2024	7.8	SQL Injection vulnerability in Super easy enterprise management system v.1.0.0 and before allows a local attacker to execute arbitrary code via a crafted script to the/ajax/Login.ashx component. **CVE ID: CVE-2024-42679**	N/A	A-CYS-SUPE-080824/394
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Aug-2024	6.1	Cross Site Scripting vulnerability in Super easy enterprise management system v.1.0.0 and before allows a local attacker to execute arbitrary code via a crafted script to the /WebSet/DlgGridSet.html component.	N/A	A-CYS-SUPE-080824/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42678		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Aug-2024	5.5	An issue in Super easy enterprise management system v.1.0.0 and before allows a local attacker to obtain the server absolute path by entering a single quotation mark. **CVE ID: CVE-2024-42680**	N/A	A-CYS-SUPE-080824/396
Vendor: datagear					
Product: datagear					
Affected Version(s): * Up to (including) 5.0.0					
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	06-Aug-2024	8.8	A vulnerability was found in DataGear up to 5.0.0. It has been declared as critical. Affected by this vulnerability is the function evaluateVariableExpression of the file ConversionSqlParamValueMapper.java of the component Data Schema Page. The manipulation leads to improper neutralization of special elements used in an expression language statement. The attack can be launched remotely. The exploit has been disclosed to	N/A	A-DAT-DATA-080824/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. The identifier VDB-273697 was assigned to this vulnerability. **CVE ID: CVE-2024-7552**		
Vendor: Dell					
Product: alienware_update					
Affected Version(s): * Up to (excluding) 5.4					
Externally Controlled Reference to a Resource in Another Sphere	06-Aug-2024	7.5	Dell Command | Update, Dell Update, and Alienware Update UWP, versions prior to 5.4, contain an Exposed Dangerous Method or Function vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to denial of service. **CVE ID: CVE-2024-28962**	https://www.dell.com/support/kbdoc/en-us/000227236/dsa-2024-169	A-DEL-ALIE-080824/398
Product: command_update					
Affected Version(s): * Up to (excluding) 5.4					
Externally Controlled Reference to a Resource in Another Sphere	06-Aug-2024	7.5	Dell Command | Update, Dell Update, and Alienware Update UWP, versions prior to 5.4, contain an Exposed Dangerous Method	https://www.dell.com/support/kbdoc/en-us/000227236/dsa-2024-169	A-DEL-COMM-080824/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or Function vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to denial of service. **CVE ID: CVE-2024-28962**		
Product: emc_idrac_service_module					
Affected Version(s): * Up to (excluding) 5.3.1.0					
Out-of-bounds Write	01-Aug-2024	4.4	Dell iDRAC Service Module version 5.3.0.0 and prior, contain an Out of bound Read Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event. **CVE ID: CVE-2024-25947**	https://www.dell.com/support/kbdoc/en-us/000227444/dsa-2024-086-security-update-for-dell-idrac-service-module-for-memory-corruption-vulnerabilities	A-DEL-EMC_-080824/400
Out-of-bounds Write	01-Aug-2024	4.4	Dell iDRAC Service Module version 5.3.0.0 and prior, contain a Out of bound Write Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	https://www.dell.com/support/kbdoc/en-us/000227444/dsa-2024-086-security-update-for-dell-idrac-service-module-for-memory-corruption-vulnerabilities	A-DEL-EMC_-080824/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-25948		
Out-of-bounds Read	01-Aug-2024	4.4	Dell iDRAC Service Module version 5.3.0.0 and prior, contain a Out of bound Read Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event. **CVE ID: CVE-2024-38481**	https://www.dell.com/support/kbdoc/en-us/000227444/dsa-2024-086-security-update-for-dell-idrac-service-module-for-memory-corruption-vulnerabilities	A-DEL-EMC_-080824/402
Out-of-bounds Write	01-Aug-2024	4.4	Dell iDRAC Service Module version 5.3.0.0 and prior contains Out of bound write Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service (partial) event. **CVE ID: CVE-2024-38489**	https://www.dell.com/support/kbdoc/en-us/000227444/dsa-2024-086-security-update-for-dell-idrac-service-module-for-memory-corruption-vulnerabilities	A-DEL-EMC_-080824/403
Out-of-bounds Write	01-Aug-2024	4.4	Dell iDRAC Service Module version 5.3.0.0 and prior, contain a Out of bound Write Vulnerability. A privileged local attacker could execute arbitrary code potentially	https://www.dell.com/support/kbdoc/en-us/000227444/dsa-2024-086-security-update-for-dell-idrac-service-module-for-memory-	A-DEL-EMC_-080824/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service event. **CVE ID: CVE-2024-38490**	corruption-vulnerabilities	
Product: update					
Affected Version(s): * Up to (excluding) 5.4					
Externally Controlled Reference to a Resource in Another Sphere	06-Aug-2024	7.5	Dell Command | Update, Dell Update, and Alienware Update UWP, versions prior to 5.4, contain an Exposed Dangerous Method or Function vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to denial of service. **CVE ID: CVE-2024-28962**	https://www.dell.com/support/kbdoc/en-us/000227236/dsa-2024-169	A-DEL-UPDA-080824/405
Vendor: deltaww					
Product: diascreen					
Affected Version(s): * Up to (excluding) 1.4.2					
Out-of-bounds Write	06-Aug-2024	7.8	A crafted DPA file could force Delta Electronics DIAScreen to overflow a stack-based buffer, which could allow an attacker to execute arbitrary code. **CVE ID: CVE-2024-7502**	N/A	A-DEL-DIAS-080824/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: devlop.systems					
Product: id4portais					
Affected Version(s): * Up to (including) 2022.837.002a					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	ID4Portais in version < V.2022.837.002a returns message parameter unsanitized in the response, resulting in a HTML Injection vulnerability. **CVE ID: CVE-2023-40819**	N/A	A-DEV-ID4P-080824/407
Vendor: dieboldnixdorf					
Product: vynamic_security_suite					
Affected Version(s): * Up to (excluding) 3.3.0sr10					
Improper Validation of Integrity Check Value	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR10 fails to validate /etc/mtab during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-24063**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/408
Affected Version(s): * Up to (excluding) 3.3.0sr12					
N/A	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR12, 4.0.0 SR04, 4.1.0 SR02, and 4.2.0 SR01 fails	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to validate the directory structure of the root file system during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-24062**		
Affected Version(s): * Up to (excluding) 3.3.0sr15					
Insufficient Verification of Data Authenticity	08-Aug-2024	6.6	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR15, 4.0.0 SR05, 4.1.0 SR03, and 4.2.0 SR02 fails to validate the directory contents of certain directories (e.g., ensuring the expected hash sum) during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-28865**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/410
Affected Version(s): * Up to (excluding) 3.3.0sr16					
Improper Validation	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security	https://www.dieboldnixdorf.co	A-DIE-VYNA-080824/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Integrity Check Value			Suite (VSS) before 3.3.0 SR16, 4.0.0 SR06, 4.1.0 SR04, 4.2.0 SR03, and 4.3.0 SR01 fails to validate symlinks during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-33206**	m/en-us/banking/portfolio/software/security/	
Affected Version(s): * Up to (excluding) 3.3.0sr17					
Improper Initialization	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR17, 4.0.0 SR07, 4.1.0 SR04, 4.2.0 SR04, and 4.3.0 SR02 fails to validate file attributes during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-40261**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/412
Affected Version(s): * Up to (excluding) 3.3.0sr4					
N/A	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before	https://www.dieboldnixdorf.com/en-	A-DIE-VYNA-080824/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.3.0 SR4 fails to validate /etc/initab during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-24064**	us/banking/portfolio/software/security/	
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.0sr04					
N/A	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR12, 4.0.0 SR04, 4.1.0 SR02, and 4.2.0 SR01 fails to validate the directory structure of the root file system during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-24062**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/414
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.0sr05					
Insufficient Verification of Data Authenticity	08-Aug-2024	6.6	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR15, 4.0.0 SR05, 4.1.0 SR03, and 4.2.0 SR02 fails	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/415

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to validate the directory contents of certain directories (e.g., ensuring the expected hash sum) during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-28865**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.0sr06					
Improper Validation of Integrity Check Value	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR16, 4.0.0 SR06, 4.1.0 SR04, 4.2.0 SR03, and 4.3.0 SR01 fails to validate symlinks during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-33206**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/416
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.0sr07					
Improper Initializatio n	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR17, 4.0.0	https://www.dieboldnixdorf.com/en-us/banking/por	A-DIE-VYNA-080824/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SR07, 4.1.0 SR04, 4.2.0 SR04, and 4.3.0 SR02 fails to validate file attributes during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-40261**	tfolio/software/security/	
Affected Version(s): From (including) 4.1.0 Up to (excluding) 4.1.0sr02					
N/A	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR12, 4.0.0 SR04, 4.1.0 SR02, and 4.2.0 SR01 fails to validate the directory structure of the root file system during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-24062**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/418
Affected Version(s): From (including) 4.1.0 Up to (excluding) 4.1.0sr03					
Insufficient Verification of Data	08-Aug-2024	6.6	Diebold Nixdorf Vynamic Security Suite (VSS) before	https://www.dieboldnixdorf.com/en-	A-DIE-VYNA-080824/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			3.3.0 SR15, 4.0.0 SR05, 4.1.0 SR03, and 4.2.0 SR02 fails to validate the directory contents of certain directories (e.g., ensuring the expected hash sum) during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-28865**	us/banking/portfolio/software/security/	
Affected Version(s): From (including) 4.1.0 Up to (excluding) 4.1.0sr04					
Improper Validation of Integrity Check Value	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR16, 4.0.0 SR06, 4.1.0 SR04, 4.2.0 SR03, and 4.3.0 SR01 fails to validate symlinks during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-33206**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Initialization	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR17, 4.0.0 SR07, 4.1.0 SR04, 4.2.0 SR04, and 4.3.0 SR02 fails to validate file attributes during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-40261**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/421
Affected Version(s): From (including) 4.2.0 Up to (excluding) 4.2.0sr01					
N/A	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR12, 4.0.0 SR04, 4.1.0 SR02, and 4.2.0 SR01 fails to validate the directory structure of the root file system during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-24062**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/422

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.2.0 Up to (excluding) 4.2.0sr02					
Insufficient Verification of Data Authenticity	08-Aug-2024	6.6	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR15, 4.0.0 SR05, 4.1.0 SR03, and 4.2.0 SR02 fails to validate the directory contents of certain directories (e.g., ensuring the expected hash sum) during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-28865**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/423
Affected Version(s): From (including) 4.2.0 Up to (excluding) 4.2.0sr03					
Improper Validation of Integrity Check Value	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR16, 4.0.0 SR06, 4.1.0 SR04, 4.2.0 SR03, and 4.3.0 SR01 fails to validate symlinks during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk.	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-33206		
Affected Version(s): From (including) 4.2.0 Up to (excluding) 4.2.0sr04					
Improper Initialization	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR17, 4.0.0 SR07, 4.1.0 SR04, 4.2.0 SR04, and 4.3.0 SR02 fails to validate file attributes during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-40261**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/425
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.3.0sr01					
Improper Validation of Integrity Check Value	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR16, 4.0.0 SR06, 4.1.0 SR04, 4.2.0 SR03, and 4.3.0 SR01 fails to validate symlinks during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk.	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/426

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-33206		
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.3.0sr03					
Improper Initialization	08-Aug-2024	6.8	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR17, 4.0.0 SR07, 4.1.0 SR04, 4.2.0 SR04, and 4.3.0 SR02 fails to validate file attributes during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk. **CVE ID: CVE-2023-40261**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/security/	A-DIE-VYNA-080824/427
Vendor: Djangoproject					
Product: django					
Affected Version(s): From (including) 4.2 Up to (excluding) 4.2.15					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2024	9.8	An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. QuerySet.values() and values_list() methods on models with a JSONField are subject to SQL injection in column aliases via a crafted JSON object key as a passed *arg.	https://docs.djangoproject.com/en/dev/releases/security/, https://www.djangoproject.com/weblog/2024/aug/06/security-releases/	A-DJA-DJAN-080824/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42005		
N/A	07-Aug-2024	7.5	An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. The floatformat template filter is subject to significant memory consumption when given a string representation of a number in scientific notation with a large exponent. **CVE ID: CVE-2024-41989**	https://docs.djangoproject.com/en/dev/releases/security/, https://www.djangoproject.com/weblog/2024/aug/06/security-releases/	A-DJA-DJAN-080824/429
N/A	07-Aug-2024	7.5	An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. The urlize() and urlizetrunc() template filters are subject to a potential denial-of-service attack via very large inputs with a specific sequence of characters. **CVE ID: CVE-2024-41990**	https://docs.djangoproject.com/en/dev/releases/security/, https://www.djangoproject.com/weblog/2024/aug/06/security-releases/	A-DJA-DJAN-080824/430
Improper Validation of Specified Quantity in Input	07-Aug-2024	7.5	An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. The urlize and urlizetrunc template filters,	https://docs.djangoproject.com/en/dev/releases/security/, https://www.djangoproject.com/weblog/202	A-DJA-DJAN-080824/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the AdminURLFieldWidget widget, are subject to a potential denial-of-service attack via certain inputs with a very large number of Unicode characters. **CVE ID: CVE-2024-41991**	4/aug/06/security-releases/	
Affected Version(s): From (including) 5.0 Up to (excluding) 5.0.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2024	9.8	An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. QuerySet.values() and values_list() methods on models with a JSONField are subject to SQL injection in column aliases via a crafted JSON object key as a passed *arg. **CVE ID: CVE-2024-42005**	https://docs.djangoproject.com/en/dev/releases/security/, https://www.djangoproject.com/weblog/2024/aug/06/security-releases/	A-DJA-DJAN-080824/432
N/A	07-Aug-2024	7.5	An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. The floatformat template filter is subject to significant memory consumption when given a string representation of a number in scientific	https://docs.djangoproject.com/en/dev/releases/security/, https://www.djangoproject.com/weblog/2024/aug/06/security-releases/	A-DJA-DJAN-080824/433

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			notation with a large exponent. **CVE ID: CVE-2024-41989**		
N/A	07-Aug-2024	7.5	An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. The urlize() and urlizetrunc() template filters are subject to a potential denial-of-service attack via very large inputs with a specific sequence of characters. **CVE ID: CVE-2024-41990**	https://docs.djangoproject.com/en/dev/releases/security/, https://www.djangoproject.com/weblog/2024/aug/06/security-releases/	A-DJA-DJAN-080824/434
Improper Validation of Specified Quantity in Input	07-Aug-2024	7.5	An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. The urlize and urlizetrunc template filters, and the AdminURLFieldWidget widget, are subject to a potential denial-of-service attack via certain inputs with a very large number of Unicode characters. **CVE ID: CVE-2024-41991**	https://docs.djangoproject.com/en/dev/releases/security/, https://www.djangoproject.com/weblog/2024/aug/06/security-releases/	A-DJA-DJAN-080824/435
Vendor: dmytropopov					
Product: light_poll					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.0.0					
Cross-Site Request Forgery (CSRF)	06-Aug-2024	8.8	The Light Poll WordPress plugin through 1.0.0 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks **CVE ID: CVE-2024-6720**	N/A	A-DMY-LIGH-080824/436
Vendor: eladmin					
Product: eladmin					
Affected Version(s): * Up to (including) 2.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2024	9.8	A vulnerability was found in elunez eladmin up to 2.7 and classified as critical. This issue affects some unknown processing of the file /api/deploy/upload /api/database/upload of the component Database Management/Deployment Management. The manipulation of the argument file leads to path traversal: 'dir/../../filename'. The exploit has been disclosed to the public and may	https://github.com/elunez/eladmin/issues/851	A-ELA-ELAD-080824/437

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. The associated identifier of this vulnerability is VDB-273551. **CVE ID: CVE-2024-7458**		
Vendor: elliptic_project					
Product: elliptic					
Affected Version(s): 6.5.6					
Improper Verification of Cryptographic Signature	02-Aug-2024	9.1	In the Elliptic package 6.5.6 for Node.js, ECDSA signature malleability occurs because BER-encoded signatures are allowed. **CVE ID: CVE-2024-42461**	https://github.com/indutny/elliptic/pull/317	A-ELL-ELLI-080824/438
Vendor: emiloimagtolis					
Product: ticket_reservation_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2024	9.8	A vulnerability classified as critical was found in itsourcecode Ticket Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file login.php of the component Login Page. The manipulation of the argument username leads to sql injection. The attack can be	N/A	A-EMI-TICK-080824/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273529 was assigned to this vulnerability. **CVE ID: CVE-2024-7444**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2024	7.2	A vulnerability, which was classified as critical, has been found in itsourcecode Ticket Reservation System 1.0. Affected by this issue is some unknown functionality of the file checkout_ticket_save.php. The manipulation of the argument data leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-273530 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-7445**	N/A	A-EMI-TICK-080824/440
Improper Neutralization of	03-Aug-2024	7.2	A vulnerability, which was classified as critical,	N/A	A-EMI-TICK-080824/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			was found in itsourcecode Ticket Reservation System 1.0. This affects an unknown part of the file list_tickets.php. The manipulation of the argument prefSeat_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273531. **CVE ID: CVE-2024-7446**		
Vendor: enjayworld					
Product: enjay_crm					
Affected Version(s): 1.0					
N/A	07-Aug-2024	7.8	An issue in the Ping feature of IT Solutions Enjay CRM OS v1.0 allows attackers to escape the restricted terminal environment and gain root-level privileges on the underlying system. **CVE ID: CVE-2024-41308**	N/A	A-ENJ-ENJA-080824/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Aug-2024	7.8	An issue in the Hardware info module of IT Solutions Enjay CRM OS v1.0 allows attackers to escape the restricted terminal environment and gain root-level privileges on the underlying system. **CVE ID: CVE-2024-41309**	N/A	A-ENJ-ENJA-080824/443
Vendor: F5					
Product: big-ip_access_policy_manager					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/444
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/446
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can	https://my.f5.com/manage/s/	A-F5-BIG--080824/447

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	article/K10438187	
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/448
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate.	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/449

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/450
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/452
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/454
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/455
Product: big-ip_advanced_firewall_manager					
Affected Version(s): 17.1.0					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/456
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/457

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/458
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/459
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/460

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/461
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/462

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/463
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/465
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization.	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/466

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/467
Product: big-ip_advanced_web_application_firewall					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/468

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39778		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/469
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/470

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/471
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/472
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server,	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/474

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/475
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/476
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/478
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/479

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**		
Product: big-ip_analytics					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/480
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate.	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/482
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/484
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/486
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/487
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/488
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/489

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/490
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/491
Product: big-ip_application_acceleration_manager					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/492

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/493
Allocation of Resources Without	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			(VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/495
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/496

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/497
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization.	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/498

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/499
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/501
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/503
Product: big-ip_application_security_manager					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/504
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server,	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/505

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/506

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/507
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/508
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/510
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/511

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/512
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate.	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/513

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/514
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/515

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41723		
Product: big-ip_application_visibility_and_reporting					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/516
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/518
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/519
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is	https://my.f5.com/manage/s/	A-F5-BIG--080824/520

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	article/K05710614	
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/521
Allocation of	14-Aug-2024	7.5	In BIG-IP tenants running on r2000	https://my.f5.com/manage/s/	A-F5-BIG--080824/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resources Without Limits or Throttling			and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	article/K00013 8833	
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/523
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate.	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/524

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/525
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/526

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/527
Product: big-ip_automation_toolchain					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/529
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization.	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/530

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/531
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/532
NULL Pointer	14-Aug-2024	7.5	When TCP profile with Multipath TCP	https://my.f5.com/manage/s/	A-F5-BIG--080824/533

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	article/K00013 8477	
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K00013 8833	A-F5-BIG--080824/534

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41727		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/535
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/536
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/538
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/539

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**		
Product: big-ip_carrier-grade_nat					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/540
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate.	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/541

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/542
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/543

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/544
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/546
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/547
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/548
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/549

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/550
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/551
Product: big-ip_container_ingress_services					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/552

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/553
Allocation of Resources Without	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			(VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/555
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/556

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/557
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization.	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/558

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/559
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/560

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/561
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/562

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/563
Product: big-ip_ddos_hybrid_defender					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/564
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server,	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/565

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/566

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/567
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/568
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/570
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/571

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/572
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate.	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/573

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/574
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/575

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41723		
Product: big-ip_domain_name_system					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/576
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/578
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/579
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is	https://my.f5.com/manage/s/	A-F5-BIG--080824/580

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	article/K05710614	
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/581
Allocation of	14-Aug-2024	7.5	In BIG-IP tenants running on r2000	https://my.f5.com/manage/s/	A-F5-BIG--080824/582

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resources Without Limits or Throttling			and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	article/K00013 8833	
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/583
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate.	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/584

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/585
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/586

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/587
Product: big-ip_edge_gateway					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/589
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization.	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/590

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/591
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/592
NULL Pointer	14-Aug-2024	7.5	When TCP profile with Multipath TCP	https://my.f5.com/manage/s/	A-F5-BIG--080824/593

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	article/K00013 8477	
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K00013 8833	A-F5-BIG--080824/594

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41727		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/595
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/596
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/598
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/599

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**		
Product: big-ip_fraud_protection_service					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/600
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate.	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/601

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/602
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/603

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/604
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/606
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/607
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/608
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/609

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/610
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/611
Product: big-ip_global_traffic_manager					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/613
Allocation of Resources Without	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			(VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/615
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/616

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/617
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization.	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/618

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/619
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/620

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/621
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/622

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/623
Product: big-ip_link_controller					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/624
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server,	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/625

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/626

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/627
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/628
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/630
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/631

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/632
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate.	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/633

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/634
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/635

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41723		
Product: big-ip_local_traffic_manager					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/636
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/638
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/639
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is	https://my.f5.com/manage/s/	A-F5-BIG--080824/640

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	article/K05710614	
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/641
Allocation of	14-Aug-2024	7.5	In BIG-IP tenants running on r2000	https://my.f5.com/manage/s/	A-F5-BIG--080824/642

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resources Without Limits or Throttling			and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	article/K00013 8833	
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/643
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate.	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/644

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/645
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/646

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/647
Product: big-ip_next_central_manager					
Affected Version(s): 20.1.0					
Insufficient Session Expiration	14-Aug-2024	8.8	The Central Manager user session refresh token does not expire when a user logs out. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID: CVE-2024-39809**	https://my.f5.com/manage/s/article/K000140111	A-F5-BIG--080824/648

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 20.1.0 Up to (excluding) 20.2.1					
Insertion of Sensitive Information into Log File	14-Aug-2024	5.5	When generating QKView of BIG-IP Next instance from the BIG-IP Next Central Manager (CM), F5 iHealth credentials will be logged in the BIG-IP Central Manager logs. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41719**	https://my.f5.com/manage/s/article/K000140006	A-F5-BIG--080824/649
Improper Authentication	14-Aug-2024	5.3	BIG-IP Next Central Manager may allow an attacker to lock out an account that has never been logged in. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-37028**	https://my.f5.com/manage/s/article/K000139938	A-F5-BIG--080824/650
Product: big-ip_next_cloud-native_network_functions					
Affected Version(s): From (including) 1.1.0 Up to (excluding) 1.2.0					
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/651

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Product: big-ip_next_service_proxy_for_kubernetes					
Affected Version(s): From (including) 1.7.0 Up to (excluding) 1.9.0					
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/652

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: big-ip_policy_enforcement_manager					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/653
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41164		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/655
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/656
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/657

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/658
Allocation of Resources Without	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/660
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate.	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/661

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/662
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/663

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/664
Product: big-ip_ssl_orchestrator					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/666
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization.	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/667

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/668
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/669
NULL Pointer	14-Aug-2024	7.5	When TCP profile with Multipath TCP	https://my.f5.com/manage/s/	A-F5-BIG--080824/670

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	article/K00013 8477	
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K00013 8833	A-F5-BIG--080824/671

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41727		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/672
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/673
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/675
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/676

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**		
Product: big-ip_webaccelerator					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/677
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate.	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/678

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/679
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/680

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/681
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**		
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/683
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/684
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/685
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/686

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/687
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/688
Product: big-ip_websafe					
Affected Version(s): 17.1.0					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/690
Allocation of Resources Without	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			(VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/692
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.1					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**		
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/694
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization.	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/695

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/696
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.5					
N/A	14-Aug-2024	7.5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39778**	https://my.f5.com/manage/s/article/K05710614	A-F5-BIG--080824/697

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	14-Aug-2024	7.5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41164**	https://my.f5.com/manage/s/article/K000138477	A-F5-BIG--080824/698
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000138833	A-F5-BIG--080824/699

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
N/A	14-Aug-2024	4.3	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41723**	https://my.f5.com/manage/s/article/K10438187	A-F5-BIG--080824/700
Product: nginx_open_source					
Affected Version(s): From (including) 1.5.13 Up to (excluding) 1.26.2					
Out-of-bounds Read	14-Aug-2024	4.7	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_mp4_module, which might allow an attacker to over-read NGINX worker memory resulting in its termination, using a specially crafted mp4 file. The issue only affects NGINX if it is built with the ngx_http_mp4_module and the mp4 directive is used in the configuration file. Additionally, the attack is possible only if an attacker can trigger	https://my.f5.com/manage/s/article/K000140529	A-F5-NGIN-080824/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the processing of a specially crafted mp4 file with the ngx_http_mp4_module. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-7347**		
Product: nginx_plus					
Affected Version(s): From (including) r27 Up to (excluding) r31					
Out-of-bounds Read	14-Aug-2024	4.7	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_mp4_module, which might allow an attacker to over-read NGINX worker memory resulting in its termination, using a specially crafted mp4 file. The issue only affects NGINX if it is built with the ngx_http_mp4_module and the mp4 directive is used in the configuration file. Additionally, the attack is possible only if an attacker can trigger the processing of a specially crafted mp4 file with the ngx_http_mp4_module. Note: Software versions which	https://my.f5.com/manage/s/article/K000140529	A-F5-NGIN-080824/702

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-7347**		
Affected Version(s): r30					
Operation on a Resource after Expiration or Release	14-Aug-2024	7.5	When the NGINX Plus is configured to use the MQTT pre-read module, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39792**	https://my.f5.com/manage/s/article/K000140108	A-F5-NGIN-080824/703
Affected Version(s): r31					
Operation on a Resource after Expiration or Release	14-Aug-2024	7.5	When the NGINX Plus is configured to use the MQTT pre-read module, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39792**	https://my.f5.com/manage/s/article/K000140108	A-F5-NGIN-080824/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Aug-2024	4.7	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_mp4_module, which might allow an attacker to over-read NGINX worker memory resulting in its termination, using a specially crafted mp4 file. The issue only affects NGINX if it is built with the ngx_http_mp4_module and the mp4 directive is used in the configuration file. Additionally, the attack is possible only if an attacker can trigger the processing of a specially crafted mp4 file with the ngx_http_mp4_module. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-7347**	https://my.f5.com/manage/s/article/K000140529	A-F5-NGIN-080824/705
Affected Version(s): r32					
Operation on a Resource after Expiration or Release	14-Aug-2024	7.5	When the NGINX Plus is configured to use the MQTT pre-read module, undisclosed requests can cause an increase in	https://my.f5.com/manage/s/article/K000140108	A-F5-NGIN-080824/706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-39792**		
Out-of-bounds Read	14-Aug-2024	4.7	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_mp4_module, which might allow an attacker to over-read NGINX worker memory resulting in its termination, using a specially crafted mp4 file. The issue only affects NGINX if it is built with the ngx_http_mp4_module and the mp4 directive is used in the configuration file. Additionally, the attack is possible only if an attacker can trigger the processing of a specially crafted mp4 file with the ngx_http_mp4_module. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000140529	A-F5-NGIN-080824/707

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7347		
Vendor: fabianros					
Product: job_portal					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	9.8	A vulnerability was found in code-projects Job Portal 1.0. It has been rated as critical. This issue affects some unknown processing of the file rw_i_nat.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7682**	N/A	A-FAB-JOB_-080824/708
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Aug-2024	9.8	A vulnerability was found in code-projects Job Portal 1.0. It has been classified as critical. Affected is an unknown function of the file logindbc.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The	N/A	A-FAB-JOB_-080824/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7808**		
Product: online_polling					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	9.8	A vulnerability was found in code-projects Online Polling 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file registeracc.php of the component Registration. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7637**	N/A	A-FAB-ONLI-080824/710
Vendor: fastadmin					
Product: fastadmin					
Affected Version(s): 1.5.0.20240328					
Improper Neutralization of Input During Web Page Generation	04-Aug-2024	4.8	A vulnerability was found in FastAdmin 1.5.0.20240328. It has been declared as problematic. This vulnerability	N/A	A-FAS-FAST-080824/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			affects unknown code of the file /[admins_url].php/general/attachment/edit/ids/4?dialog=1 of the component Attachment Management Section. The manipulation of the argument row[url]/row[imagewidth]/row[imageheight] leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273544. **CVE ID: CVE-2024-7453**		
Vendor: Ffmpeg					
Product: ffmpeg					
Affected Version(s): * Up to (excluding) 5.1.6					
Out-of-bounds Write	12-Aug-2024	8.8	A vulnerability, which was classified as critical, was found in FFmpeg up to 5.1.5. This affects the function fill_audiodata of the file /libswresample/swresample.c. The manipulation leads	N/A	A-FFM-FFMP-080824/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to heap-based buffer overflow. It is possible to initiate the attack remotely. This issue was fixed in version 6.0 by 9903ba28c28ab18dc7b7b6fb8571cc8b5caae1a6 but a backport for 5.1 was forgotten. The exploit has been disclosed to the public and may be used. Upgrading to version 5.1.6 and 6.0 9903ba28c28ab18dc7b7b6fb8571cc8b5caae1a6 is able to address this issue. It is recommended to upgrade the affected component. **CVE ID: CVE-2024-7272**		
Vendor: fortra					
Product: goanywhere_managed_file_transfer					
Affected Version(s): * Up to (excluding) 7.6.0					
Improper Authentication	14-Aug-2024	6.5	An authentication bypass vulnerability in GoAnywhere MFT prior to 7.6.0 allows Admin Users with access to the Agent Console to circumvent some permission checks	https://www.fortra.com/security/advisories/product-security/fi-2024-009	A-FOR-GOAN-080824/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when attempting to visit other pages. This could lead to unauthorized information disclosure or modification. **CVE ID: CVE-2024-25157**		
Vendor: frogcms_project					
Product: frogcms					
Affected Version(s): 0.9.5					
Cross-Site Request Forgery (CSRF)	12-Aug-2024	8.8	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/snippet/edit/3. **CVE ID: CVE-2024-42628**	N/A	A-FRO-FROG-080824/714
Cross-Site Request Forgery (CSRF)	12-Aug-2024	8.8	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/page/edit/10. **CVE ID: CVE-2024-42629**	N/A	A-FRO-FROG-080824/715
Cross-Site Request Forgery (CSRF)	12-Aug-2024	8.8	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/plugin/file_manager/create_file.	N/A	A-FRO-FROG-080824/716

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42630		
Cross-Site Request Forgery (CSRF)	12-Aug-2024	8.8	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/layout/edit/1. **CVE ID: CVE-2024-42631**	N/A	A-FRO-FROG-080824/717
Cross-Site Request Forgery (CSRF)	12-Aug-2024	8.8	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/page/add. **CVE ID: CVE-2024-42632**	N/A	A-FRO-FROG-080824/718
Cross-Site Request Forgery (CSRF)	12-Aug-2024	8.8	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/layout/delete/1 **CVE ID: CVE-2024-42623**	N/A	A-FRO-FROG-080824/719
Cross-Site Request Forgery (CSRF)	12-Aug-2024	8.8	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/page/delete/10.	N/A	A-FRO-FROG-080824/720

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42624		
Cross-Site Request Forgery (CSRF)	12-Aug-2024	8.8	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/layout/add **CVE ID: CVE-2024-42625**	N/A	A-FRO-FROG-080824/721
Cross-Site Request Forgery (CSRF)	12-Aug-2024	8.8	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/snippet/add. **CVE ID: CVE-2024-42626**	N/A	A-FRO-FROG-080824/722
Cross-Site Request Forgery (CSRF)	12-Aug-2024	8.8	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/snippet/delete/3. **CVE ID: CVE-2024-42627**	N/A	A-FRO-FROG-080824/723
Vendor: ggerganov					
Product: llama.cpp					
Affected Version(s): * Up to (excluding) b3561					
Out-of-bounds Read	12-Aug-2024	9.8	llama.cpp provides LLM inference in C/C++. The unsafe `data` pointer member in the	https://github.com/ggerganov/llama.cpp/commit/b72942fac998672a79a1ae	A-GGE-LLAM-080824/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`rpc_tensor` structure can cause arbitrary address reading. This vulnerability is fixed in b3561. **CVE ID: CVE-2024-42478**	3c03b340f7e629980b, https://github.com/ggerganov/llama.cpp/security/advisories/GHSA-5vm9-p64x-gqw9	
Out-of-bounds Write	12-Aug-2024	9.8	llama.cpp provides LLM inference in C/C++. The unsafe `data` pointer member in the `rpc_tensor` structure can cause arbitrary address writing. This vulnerability is fixed in b3561. **CVE ID: CVE-2024-42479**	https://github.com/ggerganov/llama.cpp/commit/b72942fac998672a79a1ae3c03b340f7e629980b, https://github.com/ggerganov/llama.cpp/security/advisories/GHSA-wcr5-566p-9cwj	A-GGE-LLAM-080824/725
Missing Release of Memory after Effective Lifetime	12-Aug-2024	7.5	llama.cpp provides LLM inference in C/C++. The unsafe `type` member in the `rpc_tensor` structure can cause `global-buffer-overflow`. This vulnerability may lead to memory data leakage. The vulnerability is fixed in b3561. **CVE ID: CVE-2024-42477**	https://github.com/ggerganov/llama.cpp/commit/b72942fac998672a79a1ae3c03b340f7e629980b, https://github.com/ggerganov/llama.cpp/security/advisories/GHSA-mqp6-7pv6-fqjf	A-GGE-LLAM-080824/726
Vendor: gilacms					
Product: gila_cms					
Affected Version(s): 1.10.9					
Improper Neutralizat	12-Aug-2024	5.4	A vulnerability classified as	N/A	A-GIL-GILA-080824/727

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			problematic was found in Gila CMS 1.10.9. This vulnerability affects unknown code of the file /cm/update_rows/page?id=2 of the component HTTP POST Request Handler. The manipulation of the argument content leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7657**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 127.0.6533.72					
Use After Free	06-Aug-2024	8.8	Use after free in Downloads in Google Chrome on iOS prior to 127.0.6533.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML	N/A	A-GOO-CHRO-080824/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page. (Chromium security severity: High) **CVE ID: CVE-2024-6988**		
Use After Free	06-Aug-2024	8.8	Use after free in Loader in Google Chrome prior to 127.0.6533.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-6989**	N/A	A-GOO-CHRO-080824/729
Use After Free	06-Aug-2024	8.8	Use after free in Dawn in Google Chrome prior to 127.0.6533.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-6991**	N/A	A-GOO-CHRO-080824/730
Out-of-bounds Write	06-Aug-2024	8.8	Heap buffer overflow in Layout in Google Chrome prior to 127.0.6533.72 allowed a remote attacker to potentially exploit heap corruption via	N/A	A-GOO-CHRO-080824/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-6994**		
Use After Free	06-Aug-2024	8.8	Use after free in Tabs in Google Chrome prior to 127.0.6533.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-6997**	N/A	A-GOO-CHRO-080824/732
Use After Free	06-Aug-2024	8.8	Use after free in User Education in Google Chrome prior to 127.0.6533.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-6998**	N/A	A-GOO-CHRO-080824/733

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Aug-2024	8.8	Use after free in CSS in Google Chrome prior to 127.0.6533.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-7000**	N/A	A-GOO-CHRO-080824/734
N/A	06-Aug-2024	4.7	Inappropriate implementation in Fullscreen in Google Chrome on Android prior to 127.0.6533.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-6995**	N/A	A-GOO-CHRO-080824/735
N/A	06-Aug-2024	4.3	Inappropriate implementation in FedCM in Google Chrome prior to 127.0.6533.72 allowed a remote attacker who	N/A	A-GOO-CHRO-080824/736

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-6999**		
N/A	06-Aug-2024	4.3	Inappropriate implementation in HTML in Google Chrome prior to 127.0.6533.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-7001**	N/A	A-GOO-CHRO-080824/737
N/A	06-Aug-2024	4.3	Inappropriate implementation in FedCM in Google Chrome prior to 127.0.6533.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium	N/A	A-GOO-CHRO-080824/738

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: Low) **CVE ID: CVE-2024-7003**		
N/A	06-Aug-2024	4.3	Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 127.0.6533.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass discretionary access control via a malicious file. (Chromium security severity: Low) **CVE ID: CVE-2024-7004**	N/A	A-GOO-CHRO-080824/739
N/A	06-Aug-2024	4.3	Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 127.0.6533.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass discretionary access control via a malicious file. (Chromium	N/A	A-GOO-CHRO-080824/740

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: Low) **CVE ID: CVE-2024-7005**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Aug-2024	3.1	Race in Frames in Google Chrome prior to 127.0.6533.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-6996**	N/A	A-GOO-CHRO-080824/741
Affected Version(s): * Up to (excluding) 127.0.6533.88					
Use of Uninitialized Resource	01-Aug-2024	8.8	Uninitialized Use in Dawn in Google Chrome on Android prior to 127.0.6533.88 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Critical) **CVE ID: CVE-2024-6990**	https://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-080824/742
Out-of-bounds Read	01-Aug-2024	8.8	Out of bounds read in WebTransport in Google Chrome prior to	https://chromereleases.googleblog.com/2024/07/stable-	A-GOO-CHRO-080824/743

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			127.0.6533.88 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7255**	channel-update-for-desktop_30.html	
Affected Version(s): * Up to (excluding) 127.0.6533.99					
Out-of-bounds Write	06-Aug-2024	8.8	Out of bounds memory access in ANGLE in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) **CVE ID: CVE-2024-7532**	N/A	A-GOO-CHRO-080824/744
Use After Free	06-Aug-2024	8.8	Use after free in Sharing in Google Chrome on iOS prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	N/A	A-GOO-CHRO-080824/745

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7533		
Out-of-bounds Write	06-Aug-2024	8.8	Heap buffer overflow in Layout in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7534**	N/A	A-GOO-CHRO-080824/746
Out-of-bounds Write	06-Aug-2024	8.8	Inappropriate implementation in V8 in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7535**	N/A	A-GOO-CHRO-080824/747
Use After Free	06-Aug-2024	8.8	Use after free in WebAudio in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML	N/A	A-GOO-CHRO-080824/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page. (Chromium security severity: High) **CVE ID: CVE-2024-7536**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Aug-2024	8.8	Type Confusion in V8 in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7550**	N/A	A-GOO-CHRO-080824/749
Vendor: horizoncloud					
Product: caterease					
Affected Version(s): From (including) 16.0.1.1663 Up to (including) 24.0.1.2405					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Aug-2024	9.8	An issue in Horizon Business Services Inc. Caterease 16.0.1.1663 through 24.0.1.2405 and possibly later versions, allows a remote attacker to expand control over the operating system from the database due to the execution of commands with unnecessary privileges. **CVE ID: CVE-2024-38887**	N/A	A-HOR-CATE-080824/750

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	02-Aug-2024	7.5	An issue in Horizon Business Services Inc. Caterease 16.0.1.1663 through 24.0.1.2405 and possibly later versions, allows a remote attacker to perform a Sniffing Network Traffic attack due to the cleartext transmission of sensitive information. **CVE ID: CVE-2024-38891**	N/A	A-HOR-CATE-080824/751
Vendor: IBM					
Product: infosphere_information_server					
Affected Version(s): 11.7					
N/A	15-Aug-2024	6.5	IBM InfoSphere Information Server could allow an authenticated user to consume file space resources due to unrestricted file uploads. IBM X-Force ID: 298279. **CVE ID: CVE-2024-40705**	https://www.ibm.com/support/pages/node/7160855	A-IBM-INFO-080824/752
Insufficiently Protected Credentials	15-Aug-2024	4.9	IBM InfoSphere Information Server 11.7 could allow a privileged user to obtain sensitive information from authentication request headers.	https://www.ibm.com/support/pages/node/7160853	A-IBM-INFO-080824/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 298277. **CVE ID: CVE-2024-40704**		
Affected Version(s): 11.7.0.1					
N/A	15-Aug-2024	6.5	IBM InfoSphere Information Server could allow an authenticated user to consume file space resources due to unrestricted file uploads. IBM X-Force ID: 298279. **CVE ID: CVE-2024-40705**	https://www.ibm.com/support/pages/node/7160855	A-IBM-INFO-080824/754
Insufficiently Protected Credentials	15-Aug-2024	4.9	IBM InfoSphere Information Server 11.7 could allow a privileged user to obtain sensitive information from authentication request headers. IBM X-Force ID: 298277. **CVE ID: CVE-2024-40704**	https://www.ibm.com/support/pages/node/7160853	A-IBM-INFO-080824/755
Affected Version(s): 11.7.0.2					
N/A	15-Aug-2024	6.5	IBM InfoSphere Information Server could allow an authenticated user to consume file space resources due to unrestricted file uploads. IBM X-Force ID: 298279. **CVE ID: CVE-2024-40705**	https://www.ibm.com/support/pages/node/7160855	A-IBM-INFO-080824/756

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	15-Aug-2024	4.9	IBM InfoSphere Information Server 11.7 could allow a privileged user to obtain sensitive information from authentication request headers. IBM X-Force ID: 298277. **CVE ID: CVE-2024-40704**	https://www.ibm.com/support/pages/node/7160853	A-IBM-INFO-080824/757
Vendor: isellerpal					
Product: enterprise_resource_management_system					
Affected Version(s): * Up to (including) 1.0					
Unrestricted Upload of File with Dangerous Type	15-Aug-2024	8.8	File Upload vulnerability in Huizhi enterprise resource management system v.1.0 and before allows a remote attacker to execute arbitrary code via the /nssys/common/Upload. Aspx?Action=DNPageAjaxPostBack component **CVE ID: CVE-2024-42676**	N/A	A-ISE-ENTE-080824/758
N/A	15-Aug-2024	5.5	An issue in Huizhi enterprise resource management system v.1.0 and before allows a local attacker to obtain sensitive information via the /nssys/common/fi	N/A	A-ISE-ENTE-080824/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lehandle. Aspx component **CVE ID: CVE-2024-42677**		
Vendor: itsourcecode					
Product: laravel_accounting_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	06-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in itsourcecode Laravel Accounting System 1.0. This affects an unknown part of the file app/Http/Controllers/HomeController.php. The manipulation of the argument image leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273621 was assigned to this vulnerability. **CVE ID: CVE-2024-7495**	N/A	A-ITS-LARA-080824/760
Vendor: ivanti					
Product: avalanche					
Affected Version(s): 6.3.1					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion. **CVE ID: CVE-2024-38652**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/761
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/762
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/763
Improper Restriction of XML	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche	https://forums.ivanti.com/s/article/Security-	A-IVA-AVAL-080824/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
External Entity Reference			6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/765
Affected Version(s): 6.3.1.1507					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion. **CVE ID: CVE-2024-38652**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/766
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-	A-IVA-AVAL-080824/767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/768
Improper Restriction of XML External Entity Reference	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/769
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-	A-IVA-AVAL-080824/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	
Affected Version(s): 6.3.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion. **CVE ID: CVE-2024-38652**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/771
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/772
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-	A-IVA-AVAL-080824/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	36136-CVE-2024-37399-CVE-2024-37373	
Improper Restriction of XML External Entity Reference	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/774
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/775
Affected Version(s): 6.3.2.3490					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-	A-IVA-AVAL-080824/776

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary file deletion. **CVE ID: CVE-2024-38652**	CVE-2024-37373	
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/777
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/778
Improper Restriction of XML External Entity Reference	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-	A-IVA-AVAL-080824/779

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				CVE-2024-37373	
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/780
Affected Version(s): 6.3.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion. **CVE ID: CVE-2024-38652**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/781
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-	A-IVA-AVAL-080824/782

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				CVE-2024-37373	
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/783
Improper Restriction of XML External Entity Reference	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/784
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/785
Affected Version(s): 6.3.3.101					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion. **CVE ID: CVE-2024-38652**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/786
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/787
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/788
Improper Restriction of XML	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche	https://forums.ivanti.com/s/article/Security-	A-IVA-AVAL-080824/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
External Entity Reference			6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/790
Affected Version(s): 6.3.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion. **CVE ID: CVE-2024-38652**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/791
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-	A-IVA-AVAL-080824/792

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/793
Improper Restriction of XML External Entity Reference	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/794
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-	A-IVA-AVAL-080824/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	
Affected Version(s): 6.3.4.153					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion. **CVE ID: CVE-2024-38652**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/796
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/797
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-	A-IVA-AVAL-080824/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	36136-CVE-2024-37399-CVE-2024-37373	
Improper Restriction of XML External Entity Reference	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/799
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/800
Affected Version(s): 6.4.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-	A-IVA-AVAL-080824/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary file deletion. **CVE ID: CVE-2024-38652**	CVE-2024-37373	
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/802
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/803
Improper Restriction of XML External Entity Reference	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-	A-IVA-AVAL-080824/804

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				CVE-2024-37373	
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/805
Affected Version(s): 6.4.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion. **CVE ID: CVE-2024-38652**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/806
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-	A-IVA-AVAL-080824/807

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				CVE-2024-37373	
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/808
Improper Restriction of XML External Entity Reference	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/809
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/810
Affected Version(s): 6.4.1.207					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion. **CVE ID: CVE-2024-38652**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/811
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/812
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/813
Improper Restriction of XML	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche	https://forums.ivanti.com/s/article/Security-	A-IVA-AVAL-080824/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
External Entity Reference			6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/815
Affected Version(s): 6.4.1.236					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion. **CVE ID: CVE-2024-38652**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/816
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-	A-IVA-AVAL-080824/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/818
Improper Restriction of XML External Entity Reference	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/819
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-	A-IVA-AVAL-080824/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	
Affected Version(s): 6.4.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Aug-2024	9.1	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion. **CVE ID: CVE-2024-38652**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/821
Off-by-one Error	14-Aug-2024	7.5	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS. **CVE ID: CVE-2024-36136**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/822
NULL Pointer Dereference	14-Aug-2024	7.5	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-	A-IVA-AVAL-080824/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the service, resulting in a DoS. **CVE ID: CVE-2024-37399**	36136-CVE-2024-37399-CVE-2024-37373	
Improper Restriction of XML External Entity Reference	14-Aug-2024	7.5	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server. **CVE ID: CVE-2024-38653**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/824
N/A	14-Aug-2024	7.2	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE. **CVE ID: CVE-2024-37373**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373	A-IVA-AVAL-080824/825
Product: docs\@work					
Affected Version(s): * Up to (excluding) 2.26.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Aug-2024	5.5	Ivanti Docs@Work for Android, before 2.26.0 is affected by the 'Dirty Stream' vulnerability. The application fails to properly sanitize file names, resulting in a path traversal-affiliated	https://forums.ivanti.com/s/article/Security-Advisory-CVE-2024-37403-Dirty-Stream-for-Ivanti-Docs-Work-for-Android	A-IVA-DOCS-080824/826

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This potentially enables other malicious apps on the device to read sensitive information stored in the app root. **CVE ID: CVE-2024-37403**		
Product: endpoint_manager_mobile					
Affected Version(s): * Up to (excluding) 12.1.0.1					
Improper Authentication	07-Aug-2024	9.8	An insufficient authorization vulnerability in web component of EPMM prior to 12.1.0.1 allows an unauthorized attacker within the network to execute arbitrary commands on the underlying operating system of the appliance. **CVE ID: CVE-2024-36130**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-for-Mobile-EPMM-July-2024	A-IVA-ENDP-080824/827
Deserialization of Untrusted Data	07-Aug-2024	8.8	An insecure deserialization vulnerability in web component of EPMM prior to 12.1.0.1 allows an authenticated remote attacker to execute arbitrary commands on the underlying operating system of the appliance.	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-for-Mobile-EPMM-July-2024	A-IVA-ENDP-080824/828

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36131		
Improper Authentication	07-Aug-2024	7.5	Insufficient verification of authentication controls in EPMM prior to 12.1.0.1 allows a remote attacker to bypass authentication and access sensitive resources. **CVE ID: CVE-2024-36132**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-for-Mobile-EPMM-July-2024	A-IVA-ENDP-080824/829
Improper Authentication	07-Aug-2024	6.5	An improper authentication vulnerability in web component of EPMM prior to 12.1.0.1 allows a remote malicious user to access potentially sensitive information **CVE ID: CVE-2024-34788**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-for-Mobile-EPMM-July-2024	A-IVA-ENDP-080824/830
Vendor: j4k0xb					
Product: webcrack					
Affected Version(s): * Up to (excluding) 2.14.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Aug-2024	7.8	webcrack is a tool for reverse engineering javascript. An arbitrary file write vulnerability exists in the webcrack module when processing specifically crafted malicious code on	https://github.com/j4k0xb/webcrack/commit/4bc5c6f353012ee7edc2cb39d01a728ab7426999, https://github.com/j4k0xb/webcrack/security/advisories/GH	A-J4K-WEBC-080824/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows systems. This vulnerability is triggered when using the unpack bundles feature in conjunction with the saving feature. If a module name includes a path traversal sequence with Windows path separators, an attacker can exploit this to overwrite files on the host system. This vulnerability allows an attacker to write arbitrary `.js` files to the host system, which can be leveraged to hijack legitimate Node.js modules to gain arbitrary code execution. This vulnerability has been patched in version 2.14.1. **CVE ID: CVE-2024-43373**	SA-ccqh-278p-xq6w	
Vendor: janobe					
Product: credit_card					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	06-Aug-2024	9.8	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this	N/A	A-JAN-CRED-080824/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'end' in '/admin/mod_reports/printreport.php' parameter. **CVE ID: CVE-2024-33960**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'categ' in '/admin/mod_reports/printreport.php' parameter. **CVE ID: CVE-2024-33959**	N/A	A-JAN-CRED-080824/833
Improper Neutralization of Special Elements used in an SQL Command	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by	N/A	A-JAN-CRED-080824/834

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			sending a specially crafted query to the server and retrieve all the information stored in it through the following 'code' in '/admin/mod_reservation/controller.php' parameter. **CVE ID: CVE-2024-33961**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'code' in '/admin/mod_reservation/index.php' parameter. **CVE ID: CVE-2024-33962**	N/A	A-JAN-CRED-080824/835
Improper Neutralization of Special Elements used in an SQL Command	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially	N/A	A-JAN-CRED-080824/836

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			crafted query to the server and retrieve all the information stored in it through the following 'id' in '/admin/mod_room/index.php' parameter. **CVE ID: CVE-2024-33963**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in '/admin/mod_users/index.php' parameter. **CVE ID: CVE-2024-33964**	N/A	A-JAN-CRED-080824/837
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information	N/A	A-JAN-CRED-080824/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stored in it through the following 'view' in '/tubigangarden/admin/mod_accomodation/index.php' parameter. **CVE ID: CVE-2024-33965**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'xtsearch' in '/admin/mod_reports/index.php' parameter. **CVE ID: CVE-2024-33966**	N/A	A-JAN-CRED-080824/839
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information	N/A	A-JAN-CRED-080824/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stored in it through the following 'view' in 'Attendance' and 'YearLevel' in '/AttendanceMonitoring/report/attendance_print.php' parameter. **CVE ID: CVE-2024-33967**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'Attendance' and 'YearLevel' in '/AttendanceMonitoring/report/index.php' parameter. **CVE ID: CVE-2024-33968**	N/A	A-JAN-CRED-080824/841
Improper Neutralization of Special Elements used in an SQL Command	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially	N/A	A-JAN-CRED-080824/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			crafted query to the server and retrieve all the information stored in it through the following 'id' in '/AttendanceMonitoring/department/index.php' parameter. **CVE ID: CVE-2024-33969**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'studid' in '/candidate/controller.php' parameter. **CVE ID: CVE-2024-33970**	N/A	A-JAN-CRED-080824/843
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the	N/A	A-JAN-CRED-080824/844

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server and retrieve all the information stored in it through the following 'username' in '/login.php' parameter. **CVE ID: CVE-2024-33971**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'events' in '/report/event_print.php' parameter. **CVE ID: CVE-2024-33972**	N/A	A-JAN-CRED-080824/845
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through	N/A	A-JAN-CRED-080824/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the following 'Attendance' and 'YearLevel' in '/report/attendance_print.php' parameter. **CVE ID: CVE-2024-33973**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'q', 'arrival', 'departure' and 'accomodation' parameters in '/index.php'. **CVE ID: CVE-2024-33979**	N/A	A-JAN-CRED-080824/847
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'start' parameter in	N/A	A-JAN-CRED-080824/848

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'/admin/mod_reports/printreport.php'. **CVE ID: CVE-2024-33980**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'start' parameter in '/admin/mod_reports/index.php'. **CVE ID: CVE-2024-33981**	N/A	A-JAN-CRED-080824/849
Product: debit_card_payment					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	9.8	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'end' in	N/A	A-JAN-DEBI-080824/850

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'/admin/mod_reports/printreport.php' parameter. **CVE ID: CVE-2024-33960**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'categ' in '/admin/mod_reports/printreport.php' parameter. **CVE ID: CVE-2024-33959**	N/A	A-JAN-DEBI-080824/851
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'code' in '/admin/mod_rese	N/A	A-JAN-DEBI-080824/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rvation/controller.php' parameter. **CVE ID: CVE-2024-33961**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'code' in '/admin/mod_reservation/index.php' parameter. **CVE ID: CVE-2024-33962**	N/A	A-JAN-DEBI-080824/853
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in '/admin/mod_roo	N/A	A-JAN-DEBI-080824/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			m/index.php' parameter. **CVE ID: CVE-2024-33963**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in '/admin/mod_users/index.php' parameter. **CVE ID: CVE-2024-33964**	N/A	A-JAN-DEBI-080824/855
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'view' in '/tubigangarden/admin/mod_accomo	N/A	A-JAN-DEBI-080824/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dation/index.php' parameter. **CVE ID: CVE-2024-33965**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'xtsearch' in '/admin/mod_reports/index.php' parameter. **CVE ID: CVE-2024-33966**	N/A	A-JAN-DEBI-080824/857
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'view' in 'Attendance' and 'YearLevel' in	N/A	A-JAN-DEBI-080824/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'/AttendanceMonitoring/report/attendance_print.php' parameter. **CVE ID: CVE-2024-33967**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'Attendance' and 'YearLevel' in '/AttendanceMonitoring/report/index.php' parameter. **CVE ID: CVE-2024-33968**	N/A	A-JAN-DEBI-080824/859
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in	N/A	A-JAN-DEBI-080824/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'/AttendanceMonitoring/department/index.php' parameter. **CVE ID: CVE-2024-33969**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'studid' in '/candidate/controller.php' parameter. **CVE ID: CVE-2024-33970**	N/A	A-JAN-DEBI-080824/861
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'username' in	N/A	A-JAN-DEBI-080824/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'/login.php' parameter. **CVE ID: CVE-2024-33971**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'events' in '/report/event_print.php' parameter. **CVE ID: CVE-2024-33972**	N/A	A-JAN-DEBI-080824/863
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'Attendance' and 'YearLevel' in '/report/attendanc	N/A	A-JAN-DEBI-080824/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			e_print.php' parameter. **CVE ID: CVE-2024-33973**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'q', 'arrival', 'departure' and 'accomodation' parameters in '/index.php'. **CVE ID: CVE-2024-33979**	N/A	A-JAN-DEBI-080824/865
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'start' parameter in '/admin/mod_reports/printreport.php'.	N/A	A-JAN-DEBI-080824/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33980		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'start' parameter in '/admin/mod_reports/index.php'. **CVE ID: CVE-2024-33981**	N/A	A-JAN-DEBI-080824/867
Product: paypal					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	9.8	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'end' in '/admin/mod_reports/printreport.php' parameter.	N/A	A-JAN-PAYP-080824/868

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33960		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'categ' in '/admin/mod_reports/printreport.php' parameter. **CVE ID: CVE-2024-33959**	N/A	A-JAN-PAYP-080824/869
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'code' in '/admin/mod_reservation/controller.php' parameter.	N/A	A-JAN-PAYP-080824/870

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33961		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'code' in '/admin/mod_reservation/index.php' parameter. **CVE ID: CVE-2024-33962**	N/A	A-JAN-PAYP-080824/871
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in '/admin/mod_room/index.php' parameter.	N/A	A-JAN-PAYP-080824/872

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33963		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in '/admin/mod_users/index.php' parameter. **CVE ID: CVE-2024-33964**	N/A	A-JAN-PAYP-080824/873
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'view' in '/tubigangarden/admin/mod_accomodation/index.php' parameter.	N/A	A-JAN-PAYP-080824/874

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33965		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'xtsearch' in '/admin/mod_reports/index.php' parameter. **CVE ID: CVE-2024-33966**	N/A	A-JAN-PAYP-080824/875
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'view' in 'Attendance' and 'YearLevel' in '/AttendanceMonitoring/report/atten	N/A	A-JAN-PAYP-080824/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dance_print.php' parameter. **CVE ID: CVE-2024-33967**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'Attendance' and 'YearLevel' in '/AttendanceMonitoring/report/index.php' parameter. **CVE ID: CVE-2024-33968**	N/A	A-JAN-PAYP-080824/877
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in '/AttendanceMonitoring/department/	N/A	A-JAN-PAYP-080824/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			index.php' parameter. **CVE ID: CVE-2024-33969**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'studid' in '/candidate/controller.php' parameter. **CVE ID: CVE-2024-33970**	N/A	A-JAN-PAYP-080824/879
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'username' in	N/A	A-JAN-PAYP-080824/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'/login.php' parameter. **CVE ID: CVE-2024-33971**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'events' in '/report/event_print.php' parameter. **CVE ID: CVE-2024-33972**	N/A	A-JAN-PAYP-080824/881
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'Attendance' and 'YearLevel' in '/report/attendanc	N/A	A-JAN-PAYP-080824/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			e_print.php' parameter. **CVE ID: CVE-2024-33973**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'q', 'arrival', 'departure' and 'accomodation' parameters in '/index.php'. **CVE ID: CVE-2024-33979**	N/A	A-JAN-PAYP-080824/883
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'start' parameter in '/admin/mod_reports/printreport.php'.	N/A	A-JAN-PAYP-080824/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33980		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'start' parameter in '/admin/mod_reports/index.php'. **CVE ID: CVE-2024-33981**	N/A	A-JAN-PAYP-080824/885
Product: school_attendence_monitoring_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	9.8	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'Users in '/report/printlogs.php' parameter.	N/A	A-JAN-SCHO-080824/886

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33974		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'categ' in '/admin/mod_reports/printreport.php' parameter. **CVE ID: CVE-2024-33959**	N/A	A-JAN-SCHO-080824/887
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'code' in '/admin/mod_reservation/controller.php' parameter.	N/A	A-JAN-SCHO-080824/888

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33961		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'code' in '/admin/mod_reservation/index.php' parameter. **CVE ID: CVE-2024-33962**	N/A	A-JAN-SCHO-080824/889
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in '/admin/mod_room/index.php' parameter.	N/A	A-JAN-SCHO-080824/890

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33963		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in '/admin/mod_users/index.php' parameter. **CVE ID: CVE-2024-33964**	N/A	A-JAN-SCHO-080824/891
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'view' in '/tubigangarden/admin/mod_accomodation/index.php' parameter.	N/A	A-JAN-SCHO-080824/892

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33965		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'xtsearch' in '/admin/mod_reports/index.php' parameter. **CVE ID: CVE-2024-33966**	N/A	A-JAN-SCHO-080824/893
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'view' in 'Attendance' and 'YearLevel' in '/AttendanceMonitoring/report/atten	N/A	A-JAN-SCHO-080824/894

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dance_print.php' parameter. **CVE ID: CVE-2024-33967**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'Attendance' and 'YearLevel' in '/AttendanceMonitoring/report/index.php' parameter. **CVE ID: CVE-2024-33968**	N/A	A-JAN-SCHO-080824/895
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in '/AttendanceMonitoring/department/	N/A	A-JAN-SCHO-080824/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			index.php' parameter. **CVE ID: CVE-2024-33969**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'studid' in '/candidate/controller.php' parameter. **CVE ID: CVE-2024-33970**	N/A	A-JAN-SCHO-080824/897
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'username' in	N/A	A-JAN-SCHO-080824/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'/login.php' parameter. **CVE ID: CVE-2024-33971**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'events' in '/report/event_print.php' parameter. **CVE ID: CVE-2024-33972**	N/A	A-JAN-SCHO-080824/899
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'Attendance' and 'YearLevel' in '/report/attendanc	N/A	A-JAN-SCHO-080824/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			e_print.php' parameter. **CVE ID: CVE-2024-33973**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'StudentID' parameter in '/AttendanceMonitoring/student/controller.php'. **CVE ID: CVE-2024-33982**	N/A	A-JAN-SCHO-080824/901
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'Attendance',	N/A	A-JAN-SCHO-080824/902

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'attenddate' and 'YearLevel' parameters in '/AttendanceMonitoring/report/attendance_print.php'. **CVE ID: CVE-2024-33983**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'Attendance', 'attenddate' and 'YearLevel' parameters in '/AttendanceMonitoring/report/index.php'. **CVE ID: CVE-2024-33984**	N/A	A-JAN-SCHO-080824/903
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could	N/A	A-JAN-SCHO-080824/904

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'View' parameter in '/course/index.php'. **CVE ID: CVE-2024-33985**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'View' parameter in '/department/index.php'. **CVE ID: CVE-2024-33986**	N/A	A-JAN-SCHO-080824/905
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could create a specially	N/A	A-JAN-SCHO-080824/906

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted URL and send it to a victim to obtain details of their session cookie via the 'Attendance', 'attenddate', 'YearLevel', 'eventdate', 'events', 'Users' and 'YearLevel' parameters in '/report/index.php'. **CVE ID: CVE-2024-33987**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'Attendance', 'attenddate' and 'YearLevel' parameters in '/report/attendance_print.php'. **CVE ID: CVE-2024-33988**	N/A	A-JAN-SCHO-080824/907
Product: school_event_management_system					
Affected Version(s): 1.0					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	9.8	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'Users in '/report/printlogs.php' parameter. **CVE ID: CVE-2024-33974**	N/A	A-JAN-SCHO-080824/908
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'categ' in '/admin/mod_reports/printreport.php' parameter. **CVE ID: CVE-2024-33959**	N/A	A-JAN-SCHO-080824/909

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'code' in '/admin/mod_reservation/controller.php' parameter. **CVE ID: CVE-2024-33961**	N/A	A-JAN-SCHO-080824/910
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'code' in '/admin/mod_reservation/index.php' parameter. **CVE ID: CVE-2024-33962**	N/A	A-JAN-SCHO-080824/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in '/admin/mod_room/index.php' parameter. **CVE ID: CVE-2024-33963**	N/A	A-JAN-SCHO-080824/912
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in '/admin/mod_users/index.php' parameter. **CVE ID: CVE-2024-33964**	N/A	A-JAN-SCHO-080824/913
Improper Neutralization of	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card	N/A	A-JAN-SCHO-080824/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'view' in '/tubigangarden/admin/mod_accomodation/index.php' parameter. **CVE ID: CVE-2024-33965**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'xtsearch' in '/admin/mod_reports/index.php' parameter. **CVE ID: CVE-2024-33966**	N/A	A-JAN-SCHO-080824/915
Improper Neutralization of	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card	N/A	A-JAN-SCHO-080824/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'view' in 'Attendance' and 'YearLevel' in '/AttendanceMonitoring/report/attendance_print.php' parameter. **CVE ID: CVE-2024-33967**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'Attendance' and 'YearLevel' in '/AttendanceMonitoring/report/index.php' parameter. **CVE ID: CVE-2024-33968**	N/A	A-JAN-SCHO-080824/917

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'id' in '/AttendanceMonitoring/department/index.php' parameter. **CVE ID: CVE-2024-33969**	N/A	A-JAN-SCHO-080824/918
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'studid' in '/candidate/controller.php' parameter. **CVE ID: CVE-2024-33970**	N/A	A-JAN-SCHO-080824/919

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'username' in '/login.php' parameter. **CVE ID: CVE-2024-33971**	N/A	A-JAN-SCHO-080824/920
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'events' in '/report/event_print.php' parameter. **CVE ID: CVE-2024-33972**	N/A	A-JAN-SCHO-080824/921
Improper Neutralization of	06-Aug-2024	7.5	SQL injection vulnerability in PayPal, Credit Card	N/A	A-JAN-SCHO-080824/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			and Debit Card Payment affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the following 'Attendance' and 'YearLevel' in '/report/attendance_print.php' parameter. **CVE ID: CVE-2024-33973**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'StudentID' parameter in '/AttendanceMonitoring/student/controller.php'. **CVE ID: CVE-2024-33982**	N/A	A-JAN-SCHO-080824/923

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'Attendance', 'attenddate' and 'YearLevel' parameters in '/AttendanceMonitoring/report/attendance_print.php'. **CVE ID: CVE-2024-33983**	N/A	A-JAN-SCHO-080824/924
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'Attendance', 'attenddate' and	N/A	A-JAN-SCHO-080824/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'YearLevel' parameters in '/AttendanceMonitoring/report/index.php'. **CVE ID: CVE-2024-33984**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'View' parameter in '/course/index.php'. **CVE ID: CVE-2024-33985**	N/A	A-JAN-SCHO-080824/926
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie	N/A	A-JAN-SCHO-080824/927

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via the 'View' parameter in '/department/index.php'. **CVE ID: CVE-2024-33986**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'Attendance', 'attenddate', 'YearLevel', 'eventdate', 'events', 'Users' and 'YearLevel' parameters in '/report/index.php'. **CVE ID: CVE-2024-33987**	N/A	A-JAN-SCHO-080824/928
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Attendance Monitoring System and School Event Management System affecting version 1.0. An attacker could	N/A	A-JAN-SCHO-080824/929

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			create a specially crafted URL and send it to a victim to obtain details of their session cookie via the 'Attendance', 'attenddate' and 'YearLevel' parameters in '/report/attendance_print.php'. **CVE ID: CVE-2024-33988**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Event Management System affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted javascript payload to an authenticated user and partially take over their browser session via the 'eventdate' and 'events' parameters in 'port/event_print.php'. **CVE ID: CVE-2024-33989**	N/A	A-JAN-SCHO-080824/930
Improper Neutralization of Input During Web Page Generation	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Event Management System affecting version 1.0. An	N/A	A-JAN-SCHO-080824/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker could exploit this vulnerability by sending a specially crafted javascript payload to an authenticated user and partially take over their browser session via the 'id' and 'view' parameters in '/user/index.php'. **CVE ID: CVE-2024-33990**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Event Management System affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the 'view' parameter in '/eventwinner/index.php'. **CVE ID: CVE-2024-33991**	N/A	A-JAN-SCHO-080824/932
Improper Neutralization of Input During Web Page Generation	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Event Management System affecting version 1.0. An attacker could exploit this	N/A	A-JAN-SCHO-080824/933

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability by sending a specially crafted query to the server and retrieve all the information stored in it through the 'view' parameter in '/student/index.php'. **CVE ID: CVE-2024-33992**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in School Event Management System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain their session details via the 'view' parameter in /candidate/index.php'. **CVE ID: CVE-2024-33993**	N/A	A-JAN-SCHO-080824/934
Product: young_entrepreneur_e-negosyo_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in E-Negosyo System affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve	N/A	A-JAN-YOUN-080824/935

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all the information stored in 'id' in '/admin/orders/controller.php' parameter **CVE ID: CVE-2024-33957**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2024	7.5	SQL injection vulnerability in E-Negosyo System affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted query to the server and retrieve all the information stored in 'phonenumber' in '/passwordrecover.php' parameter. **CVE ID: CVE-2024-33958**	N/A	A-JAN-YOUN-080824/936
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in E-Negosyo System affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted JavaScript payload to an authenticated user and partially take over their browser session via 'view' parameter in '/admin/products/index.php'.	N/A	A-JAN-YOUN-080824/937

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33975		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in E-Negosyo System affecting version 1.0. An attacker could exploit this vulnerability by sending a specially crafted JavaScript payload to an authenticated user and partially take over their browser session via 'id' parameter in '/admin/user/index.php'. **CVE ID: CVE-2024-33976**	N/A	A-JAN-YOUN-080824/938
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in E-Negosyo System affecting version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain their session cookie details via 'view' parameter in /admin/orders/index.php'. **CVE ID: CVE-2024-33977**	N/A	A-JAN-YOUN-080824/939
Improper Neutralization of Input During	06-Aug-2024	6.1	Cross-Site Scripting (XSS) vulnerability in E-Negosyo System affecting	N/A	A-JAN-YOUN-080824/940

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			version 1.0. An attacker could create a specially crafted URL and send it to a victim to obtain their session cookie details via 'category' parameter in '/index.php'. **CVE ID: CVE-2024-33978**		
Vendor: jayesh					
Product: online_exam_system					
Affected Version(s): 1.0					
N/A	12-Aug-2024	9.8	A Broken Access Control vulnerability was found in /admin/update.php and /admin/dashboard.php in Kashipara Online Exam System v1.0, which allows remote unauthenticated attackers to view administrator dashboard and delete valid user accounts via the direct URL access. **CVE ID: CVE-2024-40480**	N/A	A-JAY-ONLI-080824/941
Vendor: Jenkins					
Product: jenkins					
Affected Version(s): * Up to (excluding) 2.452.4					
Improper Check for	07-Aug-2024	8.8	Jenkins 2.470 and earlier, LTS 2.452.3	https://www.jenkins.io/securit	A-JEN-JENK-080824/942

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unusual or Exceptional Conditions			and earlier allows agent processes to read arbitrary files from the Jenkins controller file system by using the `ClassLoaderProxy #fetchJar` method in the Remoting library. **CVE ID: CVE-2024-43044**	y/advisory/2024-08-07/#SECURITY-3430	
Missing Authorization	07-Aug-2024	6.3	Jenkins 2.470 and earlier, LTS 2.452.3 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to access other users' "My Views". **CVE ID: CVE-2024-43045**	https://www.jenkins.io/security/advisory/2024-08-07/#SECURITY-3349	A-JEN-JENK-080824/943
Affected Version(s): * Up to (excluding) 2.471					
Improper Check for Unusual or Exceptional Conditions	07-Aug-2024	8.8	Jenkins 2.470 and earlier, LTS 2.452.3 and earlier allows agent processes to read arbitrary files from the Jenkins controller file system by using the `ClassLoaderProxy #fetchJar` method in the Remoting library. **CVE ID: CVE-2024-43044**	https://www.jenkins.io/security/advisory/2024-08-07/#SECURITY-3430	A-JEN-JENK-080824/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	07-Aug-2024	6.3	Jenkins 2.470 and earlier, LTS 2.452.3 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to access other users' "My Views". **CVE ID: CVE-2024-43045**	https://www.jenkins.io/security/advisory/2024-08-07/#SECURITY-3349	A-JEN-JENK-080824/945
Vendor: Johnsoncontrols					
Product: exacqvision_client					
Affected Version(s): * Up to (excluding) 24.06					
Inadequate Encryption Strength	01-Aug-2024	7.5	Under certain circumstances the communication between exacqVision Client and exacqVision Server will use insufficient key length and exchange **CVE ID: CVE-2024-32758**	https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories	A-JOH-EXAC-080824/946
Product: exacqvision_server					
Affected Version(s): * Up to (excluding) 24.06					
Inadequate Encryption Strength	01-Aug-2024	7.5	Under certain circumstances the communication between exacqVision Client and exacqVision Server will use insufficient key	https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories	A-JOH-EXAC-080824/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length and exchange **CVE ID: CVE-2024-32758**		
Improper Certificate Validation	01-Aug-2024	7.3	Under certain circumstances the exacqVision Server will not properly validate TLS certificates provided by connected devices. **CVE ID: CVE-2024-32865**	https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories	A-JOH-EXAC-080824/948
Product: exacqvision_web_service					
Affected Version(s): * Up to (including) 24.03					
Cross-Site Request Forgery (CSRF)	01-Aug-2024	8.8	Under certain circumstances the exacqVision Web Services may be susceptible to Cross-Site Request Forgery (CSRF) **CVE ID: CVE-2024-32863**	https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories	A-JOH-EXAC-080824/949
Cleartext Transmission of Sensitive Information	01-Aug-2024	8.1	Under certain circumstances exacqVision Web Services will not enforce secure web communications (HTTPS) **CVE ID: CVE-2024-32864**	https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories	A-JOH-EXAC-080824/950
Incorrect Comparison	01-Aug-2024	8.1	Under certain circumstances the ExacqVision Web Services does not provide sufficient	https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories	A-JOH-EXAC-080824/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protection from untrusted domains. **CVE ID: CVE-2024-32862**		
N/A	01-Aug-2024	5.7	Under certain circumstances the exacqVision Web Service can expose authentication token details within communications. **CVE ID: CVE-2024-32931**	https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories	A-JOH-EXAC-080824/952
Vendor: journyx					
Product: journyx					
Affected Version(s): 11.5.4					
Use of Hard-coded Credentials	07-Aug-2024	8.8	Password reset tokens are generated using an insecure source of randomness. Attackers who know the username of the Journyx installation user can bruteforce the password reset and change the administrator password. **CVE ID: CVE-2024-6890**	N/A	A-JOU-JOUR-080824/953
Improper Control of Generation of Code ('Code Injection')	08-Aug-2024	8.8	Attackers with a valid username and password can exploit a python code injection vulnerability during the natural login flow.	N/A	A-JOU-JOUR-080824/954

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-6891		
Improper Restriction of XML External Entity Reference	08-Aug-2024	7.5	The "soap_cgi.pyc" API handler allows the XML body of SOAP requests to contain references to external entities. This allows an unauthenticated attacker to read local files, perform server-side request forgery, and overwhelm the web server resources. **CVE ID: CVE-2024-6893**	N/A	A-JOU-JOUR-080824/955
Vendor: Jupyter					
Product: jupyterhub					
Affected Version(s): * Up to (excluding) 4.1.6					
N/A	08-Aug-2024	7.2	JupyterHub is software that allows one to create a multi-user server for Jupyter notebooks. Prior to versions 4.1.6 and 5.1.0, if a user is granted the `admin:users` scope, they may escalate their own privileges by making themselves a full admin user. The impact is relatively small in that `admin:users` is already an extremely privileged scope	https://github.com/jupyterhub/jupyterhub/commit/99e2720b0fc626cbeeca3c6337f917fdacfaa428, https://github.com/jupyterhub/jupyterhub/commit/ff2db557a85b6980f90c3158634bf924063ab8ba	A-JUP-JUPY-080824/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			only granted to trusted users. In effect, `admin:users` is equivalent to `admin=True`, which is not intended. Note that the change here only prevents escalation to the built-in JupyterHub admin role that has unrestricted permissions. It does not prevent users with e.g. `groups` permissions from granting themselves or other users permissions via group membership, which is intentional. Versions 4.1.6 and 5.1.0 fix this issue. **CVE ID: CVE-2024-41942**		
Affected Version(s): 5.0.0					
N/A	08-Aug-2024	7.2	JupyterHub is software that allows one to create a multi-user server for Jupyter notebooks. Prior to versions 4.1.6 and 5.1.0, if a user is granted the `admin:users` scope, they may escalate their own	https://github.com/jupyterhub/jupyterhub/commit/99e2720b0fc626cbeeca3c6337f917fdacfaa428, https://github.com/jupyterhub/jupyterhub/commit/ff2db557a85b6980f90c3	A-JUP-JUPY-080824/957

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges by making themselves a full admin user. The impact is relatively small in that `admin:users` is already an extremely privileged scope only granted to trusted users. In effect, `admin:users` is equivalent to `admin=True`, which is not intended. Note that the change here only prevents escalation to the built-in JupyterHub admin role that has unrestricted permissions. It does not prevent users with e.g. `groups` permissions from granting themselves or other users permissions via group membership, which is intentional. Versions 4.1.6 and 5.1.0 fix this issue. **CVE ID: CVE-2024-41942**	158634bf924063ab8ba	
Vendor: juzaweb					
Product: cms					
Affected Version(s): * Up to (including) 3.4.2					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	4.9	A vulnerability was found in juzaweb CMS up to 3.4.2. It has been classified as problematic. Affected is an unknown function of the file /admin-cp/theme/editor/default of the component Theme Editor. The manipulation leads to path traversal. 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-273696. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7551**	N/A	A-JUZ-CMS-080824/958
Vendor: K7computing					
Product: k7_ultimate_security					
Affected Version(s): * Up to (excluding) 17.0.2019					
NULL Pointer Dereference	06-Aug-2024	5.5	K7RKScan.sys in K7 Ultimate Security before 17.0.2019 allows local users to cause a denial of service (BSOD) because of a NULL	https://support.k7computing.com/index.php?/selfhelp/view-article/Advisory-issued-on-5th-aug-2024-417	A-K7C-K7_U-080824/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pointer dereference. **CVE ID: CVE-2024-36424**		
Vendor: kevinwong					
Product: online_food_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Aug-2024	9.8	A vulnerability was found in itsourcecode Online Food Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /addcategory.php. The manipulation of the argument cname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7838**	N/A	A-KEV-ONLI-080824/960
Vendor: Kingsoft					
Product: wps_office					
Affected Version(s): From (including) 12.2.0.13110 Up to (including) 12.2.0.13489					
Improper Limitation of a Pathname to a	15-Aug-2024	7.8	Improper path validation in promecefpluginhost.exe in Kingsoft WPS Office version	https://www.wps.com/whatsnew/pc/20240422/	A-KIN-WPS_-080824/961

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			ranging from 12.2.0.13110 to 12.2.0.16412 (exclusive) on Windows allows an attacker to load an arbitrary Windows library. The vulnerability was found weaponized as a single-click exploit in the form of a deceptive spreadsheet document **CVE ID: CVE-2024-7262**		
Affected Version(s): From (including) 2.2.0.13110 Up to (excluding) 12.2.0.17153					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Aug-2024	7.8	Improper path validation in promecefpluginhost.exe in Kingsoft WPS Office version ranging from 12.2.0.13110 to 12.2.0.17115 (exclusive) on Windows allows an attacker to load an arbitrary Windows library. The patch released in version 12.1.0.17119 to mitigate CVE-2024-7262 was not restrictive enough. Another parameter was not properly sanitized which leads to the	https://www.wps.com/whatsnew/pc/20240422/	A-KIN-WPS_-080824/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution of an arbitrary Windows library. **CVE ID: CVE-2024-7263**		
Vendor: Koha					
Product: koha					
Affected Version(s): * Up to (including) 23.05.00					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	9.6	Cross Site Scripting vulnerability in Koha ILS 23.05 and before allows a remote attacker to execute arbitrary code via the additonal-contents.pl component. **CVE ID: CVE-2024-28740**	N/A	A-KOH-KOHA-080824/963
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Aug-2024	7.2	An issue in Koha ILS 23.05 and before allows a remote attacker to execute arbitrary code via a crafted script to the format parameter. **CVE ID: CVE-2024-28739**	N/A	A-KOH-KOHA-080824/964
Vendor: Libtiff					
Product: libtiff					
Affected Version(s): 4.5.1					
NULL Pointer Dereference	12-Aug-2024	7.5	A null pointer dereference flaw was found in Libtiff via `tif_dirinfo.c`. This issue may allow an attacker to trigger memory	N/A	A-LIB-LIBT-080824/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocation failures through certain means, such as restricting the heap space size or injecting faults, causing a segmentation fault. This can cause an application crash, eventually leading to a denial of service. **CVE ID: CVE-2024-7006**		
Vendor: likeshop					
Product: likeshop					
Affected Version(s): * Up to (including) 2.5.7.20210811					
Authentication Bypass by Spoofing	07-Aug-2024	5.3	An IP Spoofing vulnerability has been discovered in Likeshop up to 2.5.7.20210811. This issue allows an attacker to replace their real IP address with any arbitrary IP address, specifically by adding a forged 'X-Forwarded' or 'Client-IP' header to requests. Exploiting IP spoofing, attackers can bypass account lockout mechanisms during attempts to log into admin accounts, spoof IP addresses	N/A	A-LIK-LIKE-080824/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in requests sent to the server, and impersonate IP addresses that have logged into user accounts, etc. **CVE ID: CVE-2024-41432**		
Vendor: Linuxfoundation					
Product: harbor					
Affected Version(s): * Up to (excluding) 2.9.5					
N/A	02-Aug-2024	4.3	Incorrect user permission validation in Harbor <v2.9.5 and Harbor <v2.10.3 allows authenticated users to modify configurations. **CVE ID: CVE-2024-22278**	N/A	A-LIN-HARB-080824/967
Affected Version(s): From (including) 2.10.0 Up to (excluding) 2.10.3					
N/A	02-Aug-2024	4.3	Incorrect user permission validation in Harbor <v2.9.5 and Harbor <v2.10.3 allows authenticated users to modify configurations. **CVE ID: CVE-2024-22278**	N/A	A-LIN-HARB-080824/968
Vendor: logsign					
Product: unified_secops_platform					
Affected Version(s): 6.4.11					
Improper Limitation	06-Aug-2024	6.5	Logsign Unified SecOps Platform	N/A	A-LOG-UNIF-080824/969

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Logsign Unified SecOps Platform. Authentication is required to exploit this vulnerability. The specific flaw exists within the get_response_json_result endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-24680. **CVE ID: CVE-2024-7564**		
Vendor: lopalopa					
Product: responsive_school_management_system					
Affected Version(s): 3.2.0					
Improper Neutralization of	07-Aug-2024	9.8	A SQL injection vulnerability in /smsa/teacher_logi	N/A	A-LOP-RESP-080824/970

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			n.php in Kashipara Responsive School Management System v1.0 allows an attacker to execute arbitrary SQL commands via the "username" parameter. **CVE ID: CVE-2024-41237**		
N/A	07-Aug-2024	6.5	An Incorrect Access Control vulnerability was found in /smsa/admin_teacher_register_approval.php and /smsa/admin_teacher_register_approval_submit.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view and approve Teacher registration. **CVE ID: CVE-2024-41251**	N/A	A-LOP-RESP-080824/971
N/A	07-Aug-2024	6.5	An Incorrect Access Control vulnerability was found in /smsa/admin_student_register_approval.php and /smsa/admin_student_register_appro	N/A	A-LOP-RESP-080824/972

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			val_submit.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view and approve student registration. **CVE ID: CVE-2024-41252**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2024	6.1	A Reflected Cross Site Scripting (XSS) vulnerability was found in " /smsa/teacher_login.php" in Kashipara Responsive School Management System v3.2.0, which allows remote attackers to execute arbitrary code via the "error" parameter. **CVE ID: CVE-2024-41240**	N/A	A-LOP-RESP-080824/973
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2024	6.1	A Reflected Cross Site Scripting (XSS) vulnerability was found in " /smsa/admin_login.php" in Kashipara Responsive School Management System v3.2.0, which allows remote attackers to execute arbitrary	N/A	A-LOP-RESP-080824/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code via "error" parameter. **CVE ID: CVE-2024-41241**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2024	6.1	A Reflected Cross Site Scripting (XSS) vulnerability was found in /smsa/student_login.php in Kashipara Responsive School Management System v3.2.0, which allows remote attackers to execute arbitrary code via "error" parameter. **CVE ID: CVE-2024-41242**	N/A	A-LOP-RESP-080824/975
N/A	07-Aug-2024	5.3	An Incorrect Access Control vulnerability was found in /smsa/admin_dashboard.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view administrator dashboard. **CVE ID: CVE-2024-41246**	N/A	A-LOP-RESP-080824/976
N/A	07-Aug-2024	5.3	An Incorrect Access Control vulnerability was found in	N/A	A-LOP-RESP-080824/977

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/smsa/add_class.php and /smsa/add_class_submit.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to add a new class entry. **CVE ID: CVE-2024-41247**		
N/A	07-Aug-2024	5.3	An Incorrect Access Control vulnerability was found in /smsa/add_subject.php and /smsa/add_subject_submit.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to add a new subject entry. **CVE ID: CVE-2024-41248**	N/A	A-LOP-RESP-080824/978
N/A	07-Aug-2024	5.3	An Incorrect Access Control vulnerability was found in /smsa/view_subject.php in Kashipara Responsive School Management System v3.2.0,	N/A	A-LOP-RESP-080824/979

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which allows remote unauthenticated attackers to view SUBJECT details. **CVE ID: CVE-2024-41249**		
N/A	07-Aug-2024	5.3	An Incorrect Access Control vulnerability was found in /smsa/view_marks .php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view MARKS details. **CVE ID: CVE-2024-41243**	N/A	A-LOP-RESP-080824/980
N/A	07-Aug-2024	5.3	An Incorrect Access Control vulnerability was found in /smsa/view_class. php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view CLASS details. **CVE ID: CVE-2024-41244**	N/A	A-LOP-RESP-080824/981
N/A	07-Aug-2024	5.3	An Incorrect Access Control vulnerability was	N/A	A-LOP-RESP-080824/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			found in /smsa/view_teachers.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view TEACHER details. **CVE ID: CVE-2024-41245**		
N/A	07-Aug-2024	5.3	An Incorrect Access Control vulnerability was found in /smsa/view_students.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view STUDENT details. **CVE ID: CVE-2024-41250**	N/A	A-LOP-RESP-080824/983
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2024	5.3	A SQL injection vulnerability in /smsa/student_login.php in Kashipara Responsive School Management System v1.0 allows an attacker to execute arbitrary SQL commands via the "username" parameter.	N/A	A-LOP-RESP-080824/984

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41238		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2024	4.8	A Stored Cross Site Scripting (XSS) vulnerability was found in "/smsa/add_class_submit.php" in Responsive School Management System v3.2.0, which allows remote attackers to execute arbitrary code via "class_name" parameter field. **CVE ID: CVE-2024-41239**	N/A	A-LOP-RESP-080824/985
Vendor: ltcms					
Product: ltcms					
Affected Version(s): 1.0.20					
Server-Side Request Forgery (SSRF)	13-Aug-2024	9.8	A vulnerability has been found in wanglongcn ltcms 1.0.20 and classified as critical. This vulnerability affects the function download of the file /api/test/download of the component API Endpoint. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may	N/A	A-LTC-LTCM-080824/986

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7740**		
Server-Side Request Forgery (SSRF)	13-Aug-2024	9.8	A vulnerability was found in wanglongcn ltcms 1.0.20. It has been classified as critical. Affected is the function multiDownload of the file /api/file/multiDownload of the component API Endpoint. The manipulation of the argument file leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7742**	N/A	A-LTC-LTCM-080824/987

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	13-Aug-2024	9.8	A vulnerability was found in wanglongcn ltcms 1.0.20. It has been declared as critical. Affected by this vulnerability is the function downloadUrl of the file /api/file/downloadUrl of the component API Endpoint. The manipulation of the argument file leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7743**	N/A	A-LTC-LTCM-080824/988
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Aug-2024	5.3	A vulnerability was found in wanglongcn ltcms 1.0.20 and classified as critical. This issue affects the function downloadFile of the file /api/file/downloadfile of the	N/A	A-LTC-LTCM-080824/989

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component API Endpoint. The manipulation of the argument file leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7741**		
Vendor: Matrix					
Product: matrix-react-sdk					
Affected Version(s): * Up to (excluding) 3.105.1					
N/A	06-Aug-2024	6.5	matrix-react-sdk is a react-based SDK for inserting a Matrix chat/voip client into a web page. A malicious homeserver could manipulate a user's account data to cause the client to enable URL previews in end-to-end encrypted rooms, in which case any URLs in encrypted messages would be sent to the server. This was patched in matrix-react-sdk	https://github.com/matrix-org/matrix-react-sdk/security/advisories/GHSA-f83w-wqhc-cfp4	A-MAT-MATR-080824/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.105.0. Deployments that trust their homeservers, as well as closed federations of trusted servers, are not affected. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2024-42347**		
Vendor: mayurik					
Product: advocate_office_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	9.8	A vulnerability classified as critical has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This affects an unknown part of the file delete_client.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7638**	N/A	A-MAY-ADVO-080824/991

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	9.8	A vulnerability classified as critical was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This vulnerability affects unknown code of the file delete_act.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7639**	N/A	A-MAY-ADVO-080824/992
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This issue affects some unknown processing of the file delete_register.php. The manipulation of the argument case_register_id leads to sql injection. The attack may be	N/A	A-MAY-ADVO-080824/993

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7640**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected is an unknown function of the file deactivate_act.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. **CVE ID: CVE-2024-7641**	N/A	A-MAY-ADVO-080824/994
Improper Neutralization of Special Elements used in an SQL Command	12-Aug-2024	9.8	A vulnerability has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0 and classified as critical. Affected by this vulnerability is an	N/A	A-MAY-ADVO-080824/995

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			unknown functionality of the file activate_act.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7642**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	5.4	A vulnerability classified as problematic has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected is an unknown function of the file addcase_stage.php. The manipulation of the argument cname leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7683**	N/A	A-MAY-ADVO-080824/996

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	5.4	A vulnerability classified as problematic was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected by this vulnerability is an unknown functionality of the file add_act.php. The manipulation of the argument aname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7684**	N/A	A-MAY-ADVO-080824/997
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	5.4	A vulnerability, which was classified as problematic, has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected by this issue is some unknown functionality of the file adds.php. The manipulation of the argument	N/A	A-MAY-ADVO-080824/998

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			name/dob/email/ mobile/address leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7685**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	5.4	A vulnerability, which was classified as problematic, was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This affects an unknown part of the file register_case.php. The manipulation of the argument title/description/opposite_lawyer leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7686**	N/A	A-MAY-ADVO-080824/999
Product: best_house_rental_management					
Affected Version(s): 1.0					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	12-Aug-2024	8	A Cross-Site Request Forgery (CSRF) vulnerability was found in SourceCodester Best House Rental Management System v1.0. This could lead to an attacker tricking the administrator into adding/modifying/deleting valid tenant data via a crafted HTML page, as demonstrated by a Delete Tenant action at the /rental/ajax.php?action=delete_tenant. **CVE ID: CVE-2024-40476**	N/A	A-MAY-BEST-080824/1000
Product: best_house_rental_management_system					
Affected Version(s): 1.0					
N/A	12-Aug-2024	8.8	SourceCodester Best House Rental Management System v1.0 is vulnerable to Incorrect Access Control via /rental/payment_report.php, /rental/balance_report.php, /rental/invoices.php, /rental/tenants.ph	N/A	A-MAY-BEST-080824/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			p, and /rental/users.php. **CVE ID: CVE-2024-40475**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	5.4	A Stored Cross Site Scripting (XSS) vulnerability was found in "manage_houses.php" in SourceCodester Best House Rental Management System v1.0. It allows remote attackers to execute arbitrary code via "House_no" and "Description" parameter fields. **CVE ID: CVE-2024-40473**	N/A	A-MAY-BEST-080824/1002
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	5.4	A Reflected Cross Site Scripting (XSS) vulnerability was found in "edit-cate.php" in SourceCodester House Rental Management System v1.0. **CVE ID: CVE-2024-40474**	N/A	A-MAY-BEST-080824/1003
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Aug-2024	5.4	A vulnerability classified as problematic was found in SourceCodester Best House Rental Management System 1.0. This	N/A	A-MAY-BEST-080824/1004

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects unknown code of the file /rental_0/rental/ajax.php?action=save_tenant of the component POST Parameter Handler. The manipulation of the argument lastname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7812**		
Vendor: Microchip					
Product: advanced_software_framework					
Affected Version(s): * Up to (including) 3.52.0.2574					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Aug-2024	9.8	Improper Input Validation vulnerability in Microchip Techology Advanced Software Framework example DHCP server can cause remote code execution through a buffer overflow. This vulnerability is associated with program files tinydhcpserver.C and program routines	https://www.microchip.com/en-us/tools-resources/develop/libraries/advanced-software-framework	A-MIC-ADVA-080824/1005

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lwip_dhcp_find_option. This issue affects Advanced Software Framework: through 3.52.0.2574. ASF is no longer being supported. Apply provided workaround or migrate to an actively maintained framework. **CVE ID: CVE-2024-7490**		
Vendor: Microsoft					
Product: .net					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.0.8					
N/A	13-Aug-2024	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID: CVE-2024-38168**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38168	A-MIC-.NET-080824/1006
N/A	13-Aug-2024	6.5	.NET and Visual Studio Information Disclosure Vulnerability **CVE ID: CVE-2024-38167**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38167	A-MIC-.NET-080824/1007
Product: 365_apps					
Affected Version(s): -					
N/A	13-Aug-2024	8.8	Microsoft Project Remote Code	https://msrc.microsoft.com/up	A-MIC-365_-080824/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38189**	date-guide/vulnerability/CVE-2024-38189	
N/A	13-Aug-2024	7.8	Microsoft Office Visio Remote Code Execution Vulnerability **CVE ID: CVE-2024-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38169	A-MIC-365_-080824/1009
N/A	13-Aug-2024	7.8	Microsoft PowerPoint Remote Code Execution Vulnerability **CVE ID: CVE-2024-38171**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38171	A-MIC-365_-080824/1010
N/A	13-Aug-2024	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID: CVE-2024-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38172	A-MIC-365_-080824/1011
N/A	13-Aug-2024	7.1	Microsoft Excel Remote Code Execution Vulnerability **CVE ID: CVE-2024-38170**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38170	A-MIC-365_-080824/1012
N/A	13-Aug-2024	6.7	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID: CVE-2024-38173**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38173	A-MIC-365_-080824/1013
N/A	12-Aug-2024	6.5	Microsoft Office Spoofing Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	A-MIC-365_-080824/1014

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38200	lity/CVE-2024-38200	
Product: app_installer					
Affected Version(s): * Up to (excluding) 1.22.11261.0					
N/A	13-Aug-2024	7.8	Windows App Installer Spoofing Vulnerability **CVE ID: CVE-2024-38177**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38177	A-MIC-APP_-080824/1015
Product: azure_connected_machine_agent					
Affected Version(s): * Up to (excluding) 1.44					
N/A	13-Aug-2024	7.8	Azure Connected Machine Agent Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38098**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38098	A-MIC-AZUR-080824/1016
N/A	13-Aug-2024	7.8	Azure Connected Machine Agent Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38162**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38162	A-MIC-AZUR-080824/1017
Product: azure_cyclecloud					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.6.3					
N/A	13-Aug-2024	7.8	Azure CycleCloud Remote Code Execution Vulnerability **CVE ID: CVE-2024-38195**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38195	A-MIC-AZUR-080824/1018
Product: azure_health_bot					
Affected Version(s): -					
Server-Side	13-Aug-2024	8.8	An authenticated attacker can exploit	https://msrc.microsoft.com/up	A-MIC-AZUR-080824/1019

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (SSRF)			an Server-Side Request Forgery (SSRF) vulnerability in Microsoft Azure Health Bot to elevate privileges over a network. **CVE ID: CVE-2024-38109**	date-guide/vulnerability/CVE-2024-38109	
Product: azure_iot_hub_device_client_sdk					
Affected Version(s): * Up to (excluding) 1.12.1					
N/A	13-Aug-2024	7	Azure IoT SDK Remote Code Execution Vulnerability **CVE ID: CVE-2024-38157**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38157	A-MIC-AZUR-080824/1020
N/A	13-Aug-2024	7	Azure IoT SDK Remote Code Execution Vulnerability **CVE ID: CVE-2024-38158**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38158	A-MIC-AZUR-080824/1021
Product: azure_stack_hub					
Affected Version(s): * Up to (excluding) 1.2311.1.22					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Aug-2024	9.3	Azure Stack Hub Spoofing Vulnerability **CVE ID: CVE-2024-38108**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38108	A-MIC-AZUR-080824/1022
N/A	13-Aug-2024	7	Azure Stack Hub Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38201	A-MIC-AZUR-080824/1023

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38201		
Product: copilot_studio					
Affected Version(s): -					
Server-Side Request Forgery (SSRF)	06-Aug-2024	6.5	An authenticated attacker can bypass Server-Side Request Forgery (SSRF) protection in Microsoft Copilot Studio to leak sensitive information over a network. **CVE ID: CVE-2024-38206**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38206	A-MIC-COPI-080824/1024
Product: dynamics_365					
Affected Version(s): 9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Aug-2024	8.2	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID: CVE-2024-38211**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38211	A-MIC-DYNA-080824/1025
Product: dynamics_crm_service_portal_web_resource					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	An unauthenticated attacker can exploit improper neutralization of input during web page generation in Microsoft Dynamics 365 to spoof over a network by tricking a user to click on a link.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38166	A-MIC-DYNA-080824/1026

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38166		
Product: office					
Affected Version(s): 2016					
N/A	12-Aug-2024	6.5	Microsoft Office Spoofing Vulnerability **CVE ID: CVE-2024-38200**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200	A-MIC-OFFI-080824/1027
Affected Version(s): 2019					
N/A	13-Aug-2024	8.8	Microsoft Project Remote Code Execution Vulnerability **CVE ID: CVE-2024-38189**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189	A-MIC-OFFI-080824/1028
N/A	13-Aug-2024	7.8	Microsoft Office Visio Remote Code Execution Vulnerability **CVE ID: CVE-2024-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38169	A-MIC-OFFI-080824/1029
N/A	13-Aug-2024	7.8	Microsoft PowerPoint Remote Code Execution Vulnerability **CVE ID: CVE-2024-38171**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38171	A-MIC-OFFI-080824/1030
N/A	13-Aug-2024	6.7	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID: CVE-2024-38173**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38173	A-MIC-OFFI-080824/1031
N/A	12-Aug-2024	6.5	Microsoft Office Spoofing Vulnerability	https://msrc.microsoft.com/update-	A-MIC-OFFI-080824/1032

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38200	guide/vulnerability/CVE-2024-38200	
Product: officeplus					
Affected Version(s): * Up to (excluding) 3.2.0.27546					
N/A	13-Aug-2024	7.8	Microsoft OfficePlus Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38084**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38084	A-MIC-OFFI-080824/1033
Product: office_long_term_servicing_channel					
Affected Version(s): 2021					
N/A	13-Aug-2024	8.8	Microsoft Project Remote Code Execution Vulnerability **CVE ID: CVE-2024-38189**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189	A-MIC-OFFI-080824/1034
N/A	13-Aug-2024	7.8	Microsoft Office Visio Remote Code Execution Vulnerability **CVE ID: CVE-2024-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38169	A-MIC-OFFI-080824/1035
N/A	13-Aug-2024	7.8	Microsoft PowerPoint Remote Code Execution Vulnerability **CVE ID: CVE-2024-38171**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38171	A-MIC-OFFI-080824/1036
N/A	13-Aug-2024	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID: CVE-2024-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38172	A-MIC-OFFI-080824/1037

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.1	Microsoft Excel Remote Code Execution Vulnerability **CVE ID: CVE-2024-38170**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38170	A-MIC-OFFI-080824/1038
N/A	13-Aug-2024	6.7	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID: CVE-2024-38173**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38173	A-MIC-OFFI-080824/1039
N/A	12-Aug-2024	6.5	Microsoft Office Spoofing Vulnerability **CVE ID: CVE-2024-38200**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200	A-MIC-OFFI-080824/1040
Product: outlook					
Affected Version(s): 2016					
N/A	13-Aug-2024	6.7	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID: CVE-2024-38173**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38173	A-MIC-OUTL-080824/1041
Product: powerpoint					
Affected Version(s): 2016					
N/A	13-Aug-2024	7.8	Microsoft PowerPoint Remote Code Execution Vulnerability **CVE ID: CVE-2024-38171**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38171	A-MIC-POWE-080824/1042
Product: project_2016					
Affected Version(s): * Up to (excluding) 16.0.5461.1001					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	8.8	Microsoft Project Remote Code Execution Vulnerability **CVE ID: CVE-2024-38189**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189	A-MIC-PROJ-080824/1043
Product: remote_desktop					
Affected Version(s): * Up to (excluding) 1.2.5560.0					
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	A-MIC-REMO-080824/1044
Product: teams					
Affected Version(s): * Up to (excluding) 7.13.0					
N/A	13-Aug-2024	6.5	Microsoft Teams for iOS Spoofing Vulnerability **CVE ID: CVE-2024-38197**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38197	A-MIC-TEAM-080824/1045
Product: visual_studio_2022					
Affected Version(s): From (including) 17.10.0 Up to (excluding) 17.10.6					
N/A	13-Aug-2024	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID: CVE-2024-38168**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38168	A-MIC-VISU-080824/1046
N/A	13-Aug-2024	6.5	.NET and Visual Studio Information Disclosure Vulnerability **CVE ID: CVE-2024-38167**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38167	A-MIC-VISU-080824/1047
Affected Version(s): From (including) 17.6.0 Up to (excluding) 17.6.18					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID: CVE-2024-38168**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38168	A-MIC-VISU-080824/1048
N/A	13-Aug-2024	6.5	.NET and Visual Studio Information Disclosure Vulnerability **CVE ID: CVE-2024-38167**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38167	A-MIC-VISU-080824/1049
Affected Version(s): From (including) 17.8.0 Up to (excluding) 17.8.13					
N/A	13-Aug-2024	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID: CVE-2024-38168**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38168	A-MIC-VISU-080824/1050
N/A	13-Aug-2024	6.5	.NET and Visual Studio Information Disclosure Vulnerability **CVE ID: CVE-2024-38167**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38167	A-MIC-VISU-080824/1051
Vendor: Mongodb					
Product: mongodb					
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.16					
N/A	13-Aug-2024	5.3	"Hot" backup files may be downloaded by underprivileged users, if they are capable of acquiring a unique backup identifier. This issue affects MongoDB Enterprise Server v6.0 versions prior	https://jira.mongodb.org/browse/SERVER-93516	A-MON-MONG-080824/1052

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to 6.0.16, MongoDB Enterprise Server v7.0 versions prior to 7.0.11 and MongoDB Enterprise Server v7.3 versions prior to 7.3.3 **CVE ID: CVE-2024-6384**		
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.11					
N/A	13-Aug-2024	5.3	"Hot" backup files may be downloaded by underprivileged users, if they are capable of acquiring a unique backup identifier. This issue affects MongoDB Enterprise Server v6.0 versions prior to 6.0.16, MongoDB Enterprise Server v7.0 versions prior to 7.0.11 and MongoDB Enterprise Server v7.3 versions prior to 7.3.3 **CVE ID: CVE-2024-6384**	https://jira.mongodb.org/browse/SERVER-93516	A-MON-MONG-080824/1053
Affected Version(s): From (including) 7.3.0 Up to (excluding) 7.3.3					
N/A	13-Aug-2024	5.3	"Hot" backup files may be downloaded by underprivileged users, if they are capable of acquiring a unique backup identifier.	https://jira.mongodb.org/browse/SERVER-93516	A-MON-MONG-080824/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects MongoDB Enterprise Server v6.0 versions prior to 6.0.16, MongoDB Enterprise Server v7.0 versions prior to 7.0.11 and MongoDB Enterprise Server v7.3 versions prior to 7.3.3 **CVE ID: CVE-2024-6384**		
Vendor: monospace					
Product: directus					
Affected Version(s): 10.13.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Aug-2024	5.4	Directus v10.13.0 allows an authenticated external attacker to execute arbitrary JavaScript on the client. This is possible because the application injects an attacker-controlled parameter that will be stored in the server and used by the client into an unsanitized DOM element. When chained with CVE-2024-6534, it could result in account takeover. **CVE ID: CVE-2024-6533**	N/A	A-MON-DIRE-080824/1055

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization Bypass Through User-Controlled Key	15-Aug-2024	4.3	Directus v10.13.0 allows an authenticated external attacker to modify presets created by the same user to assign them to another user. This is possible because the application only validates the user parameter in the 'POST /presets' request but not in the PATCH request. When chained with CVE-2024-6533, it could result in account takeover. **CVE ID: CVE-2024-6534**	N/A	A-MON-DIRE-080824/1056
Vendor: Mozilla					
Product: firefox					
Affected Version(s): * Up to (excluding) 129					
N/A	06-Aug-2024	6.5	Select options could obscure the fullscreen notification dialog. This could be used by a malicious site to perform a spoofing attack. This vulnerability affects Firefox < 129, Firefox ESR < 128.1, and Thunderbird < 128.1. **CVE ID: CVE-2024-7518**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1057

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 129.0					
Out-of-bounds Write	06-Aug-2024	9.6	Insufficient checks when processing graphics shared memory could have led to memory corruption. This could be leveraged by an attacker to perform a sandbox escape. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7519**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1058
Access of Resource Using Incompatible Type ('Type Confusion')	06-Aug-2024	8.8	A type confusion bug in WebAssembly could be leveraged by an attacker to potentially achieve code execution. This vulnerability affects Firefox < 129, Firefox ESR < 128.1, and Thunderbird < 128.1. **CVE ID: CVE-2024-7520**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1059
Improper Handling of Exceptional Conditions	06-Aug-2024	8.8	Incomplete WebAssembly exception handing could have led to a use-after-free. This	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.m	A-MOZ-FIRE-080824/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7521**	ozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	
Out-of-bounds Read	06-Aug-2024	8.8	Editor code failed to check an attribute value. This could have led to an out-of-bounds read. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7522**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1061
Use After Free	06-Aug-2024	8.8	Unexpected marking work at the start of sweeping could have led to a use-after-free. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/secur	A-MOZ-FIRE-080824/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.14. **CVE ID: CVE-2024-7527**	ity/advisories/mfsa2024-37/	
Use After Free	06-Aug-2024	8.8	Incorrect garbage collection interaction in IndexedDB could have led to a use-after-free. This vulnerability affects Firefox < 129, Firefox ESR < 128.1, and Thunderbird < 128.1. **CVE ID: CVE-2024-7528**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1063
Use After Free	06-Aug-2024	8.8	Incorrect garbage collection interaction could have led to a use-after-free. This vulnerability affects Firefox < 129. **CVE ID: CVE-2024-7530**	https://www.mozilla.org/security/advisories/mfsa2024-33/	A-MOZ-FIRE-080824/1064
Incorrect Default Permissions	06-Aug-2024	8.1	It was possible for a web extension with minimal permissions to create a `StreamFilter` which could be used to read and modify the response body of requests on any site. This vulnerability affects Firefox <	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/secur	A-MOZ-FIRE-080824/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7525**	ity/advisories/mfsa2024-37/	
Use of Uninitialized Resource	06-Aug-2024	6.5	ANGLE failed to initialize parameters which led to reading from uninitialized memory. This could be leveraged to leak sensitive data from memory. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7526**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1066
N/A	06-Aug-2024	6.5	The date picker could partially obscure security prompts. This could be used by a malicious site to trick a user into granting permissions. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1,	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/secur	A-MOZ-FIRE-080824/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7529**	ity/advisories/mfsa2024-37/	
N/A	06-Aug-2024	6.5	Calling `PK11_Encrypt()` in NSS using CKM_CHACHA20 and the same buffer for input and output can result in plaintext on an Intel Sandy Bridge processor. In Firefox this only affects the QUIC header protection feature when the connection is using the ChaCha20-Poly1305 cipher suite. The most likely outcome is connection failure, but if the connection persists despite the high packet loss it could be possible for a network observer to identify packets as coming from the same source despite a network path change. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, and Firefox ESR < 128.1.	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/	A-MOZ-FIRE-080824/1068

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7531		
Product: firefox_esr					
Affected Version(s): * Up to (excluding) 115.14.0					
Out-of-bounds Write	06-Aug-2024	9.6	Insufficient checks when processing graphics shared memory could have led to memory corruption. This could be leveraged by an attacker to perform a sandbox escape. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7519**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1069
Improper Handling of Exceptional Conditions	06-Aug-2024	8.8	Incomplete WebAssembly exception handing could have led to a use-after-free. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7521**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Aug-2024	8.8	Editor code failed to check an attribute value. This could have led to an out-of-bounds read. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7522**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1071
Use After Free	06-Aug-2024	8.8	Unexpected marking work at the start of sweeping could have led to a use-after-free. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7527**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1072
Incorrect Default Permissions	06-Aug-2024	8.1	It was possible for a web extension with minimal permissions to create a `StreamFilter` which could be used to read and modify the	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.m	A-MOZ-FIRE-080824/1073

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response body of requests on any site. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7525**	ozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	
Use of Uninitialized Resource	06-Aug-2024	6.5	ANGLE failed to initialize parameters which led to reading from uninitialized memory. This could be leveraged to leak sensitive data from memory. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7526**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1074
N/A	06-Aug-2024	6.5	The date picker could partially obscure security prompts. This could be used by a malicious site to trick a user into granting permissions. This	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.m	A-MOZ-FIRE-080824/1075

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7529**	ozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	
N/A	06-Aug-2024	6.5	Calling `PK11_Encrypt()` in NSS using CKM_CHACHA20 and the same buffer for input and output can result in plaintext on an Intel Sandy Bridge processor. In Firefox this only affects the QUIC header protection feature when the connection is using the ChaCha20-Poly1305 cipher suite. The most likely outcome is connection failure, but if the connection persists despite the high packet loss it could be possible for a network observer to identify packets as coming from the same source despite a network path change. This vulnerability	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/	A-MOZ-FIRE-080824/1076

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Firefox < 129, Firefox ESR < 115.14, and Firefox ESR < 128.1. **CVE ID: CVE-2024-7531**		
Affected Version(s): * Up to (excluding) 128.1					
N/A	06-Aug-2024	6.5	Select options could obscure the fullscreen notification dialog. This could be used by a malicious site to perform a spoofing attack. This vulnerability affects Firefox < 129, Firefox ESR < 128.1, and Thunderbird < 128.1. **CVE ID: CVE-2024-7518**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1077
Affected Version(s): * Up to (excluding) 128.1.0					
Access of Resource Using Incompatible Type ('Type Confusion')	06-Aug-2024	8.8	A type confusion bug in WebAssembly could be leveraged by an attacker to potentially achieve code execution. This vulnerability affects Firefox < 129, Firefox ESR < 128.1, and Thunderbird < 128.1. **CVE ID: CVE-2024-7520**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1078
Use After Free	06-Aug-2024	8.8	Incorrect garbage collection	https://www.mozilla.org/secur	A-MOZ-FIRE-080824/1079

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in IndexedDB could have led to a use-after-free. This vulnerability affects Firefox < 129, Firefox ESR < 128.1, and Thunderbird < 128.1. **CVE ID: CVE-2024-7528**	ity/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	
Affected Version(s): 128.0					
Out-of-bounds Write	06-Aug-2024	9.6	Insufficient checks when processing graphics shared memory could have led to memory corruption. This could be leveraged by an attacker to perform a sandbox escape. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7519**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1080
Improper Handling of Exceptional Conditions	06-Aug-2024	8.8	Incomplete WebAssembly exception handing could have led to a use-after-free. This vulnerability affects Firefox < 129, Firefox ESR <	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/,	A-MOZ-FIRE-080824/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7521**	https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	
Out-of-bounds Read	06-Aug-2024	8.8	Editor code failed to check an attribute value. This could have led to an out-of-bounds read. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7522**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1082
Use After Free	06-Aug-2024	8.8	Unexpected marking work at the start of sweeping could have led to a use-after-free. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7527**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	06-Aug-2024	8.1	It was possible for a web extension with minimal permissions to create a `StreamFilter` which could be used to read and modify the response body of requests on any site. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7525**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1084
Use of Uninitialized Resource	06-Aug-2024	6.5	ANGLE failed to initialize parameters which led to reading from uninitialized memory. This could be leveraged to leak sensitive data from memory. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7526**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1085

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Aug-2024	6.5	The date picker could partially obscure security prompts. This could be used by a malicious site to trick a user into granting permissions. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7529**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-FIRE-080824/1086
N/A	06-Aug-2024	6.5	Calling `PK11_Encrypt()` in NSS using CKM_CHACHA20 and the same buffer for input and output can result in plaintext on an Intel Sandy Bridge processor. In Firefox this only affects the QUIC header protection feature when the connection is using the ChaCha20-Poly1305 cipher suite. The most likely outcome is connection failure, but if the connection persists despite the high	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/	A-MOZ-FIRE-080824/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet loss it could be possible for a network observer to identify packets as coming from the same source despite a network path change. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, and Firefox ESR < 128.1. **CVE ID: CVE-2024-7531**		
Product: thunderbird					
Affected Version(s): * Up to (excluding) 115.14.0					
Out-of-bounds Write	06-Aug-2024	9.6	Insufficient checks when processing graphics shared memory could have led to memory corruption. This could be leveraged by an attacker to perform a sandbox escape. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7519**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1088
Improper Handling of Exceptiona	06-Aug-2024	8.8	Incomplete WebAssembly exception handing could have led to a	https://www.mozilla.org/security/advisories/mfsa2024-33/,	A-MOZ-THUN-080824/1089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			use-after-free. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7521**	https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	
Out-of-bounds Read	06-Aug-2024	8.8	Editor code failed to check an attribute value. This could have led to an out-of-bounds read. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7522**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1090
Use After Free	06-Aug-2024	8.8	Unexpected marking work at the start of sweeping could have led to a use-after-free. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/secur	A-MOZ-THUN-080824/1091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.14. **CVE ID: CVE-2024-7527**	ity/advisories/mfsa2024-37/	
Incorrect Default Permissions	06-Aug-2024	8.1	It was possible for a web extension with minimal permissions to create a `StreamFilter` which could be used to read and modify the response body of requests on any site. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7525**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1092
Use of Uninitialized Resource	06-Aug-2024	6.5	ANGLE failed to initialize parameters which led to reading from uninitialized memory. This could be leveraged to leak sensitive data from memory. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/secur	A-MOZ-THUN-080824/1093

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.14. **CVE ID: CVE-2024-7526**	ity/advisories/mfsa2024-37/	
N/A	06-Aug-2024	6.5	The date picker could partially obscure security prompts. This could be used by a malicious site to trick a user into granting permissions. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7529**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1094
Affected Version(s): * Up to (excluding) 128.1					
N/A	06-Aug-2024	6.5	Select options could obscure the fullscreen notification dialog. This could be used by a malicious site to perform a spoofing attack. This vulnerability affects Firefox < 129, Firefox ESR < 128.1, and Thunderbird < 128.1. **CVE ID: CVE-2024-7518**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 128.1.0					
Access of Resource Using Incompatible Type ('Type Confusion')	06-Aug-2024	8.8	A type confusion bug in WebAssembly could be leveraged by an attacker to potentially achieve code execution. This vulnerability affects Firefox < 129, Firefox ESR < 128.1, and Thunderbird < 128.1. **CVE ID: CVE-2024-7520**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1096
Use After Free	06-Aug-2024	8.8	Incorrect garbage collection interaction in IndexedDB could have led to a use-after-free. This vulnerability affects Firefox < 129, Firefox ESR < 128.1, and Thunderbird < 128.1. **CVE ID: CVE-2024-7528**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1097
Affected Version(s): 128.0.1					
Out-of-bounds Write	06-Aug-2024	9.6	Insufficient checks when processing graphics shared memory could have led to memory corruption. This could be leveraged by an attacker to perform a sandbox escape. This vulnerability	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/	A-MOZ-THUN-080824/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7519**	mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	
Improper Handling of Exceptional Conditions	06-Aug-2024	8.8	Incomplete WebAssembly exception handing could have led to a use-after-free. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7521**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1099
Out-of-bounds Read	06-Aug-2024	8.8	Editor code failed to check an attribute value. This could have led to an out-of-bounds read. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14.	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1100

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7522		
Use After Free	06-Aug-2024	8.8	Unexpected marking work at the start of sweeping could have led to a use-after-free. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7527**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1101
Incorrect Default Permissions	06-Aug-2024	8.1	It was possible for a web extension with minimal permissions to create a `StreamFilter` which could be used to read and modify the response body of requests on any site. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7525**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1102

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	06-Aug-2024	6.5	ANGLE failed to initialize parameters which led to reading from uninitialized memory. This could be leveraged to leak sensitive data from memory. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7526**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1103
N/A	06-Aug-2024	6.5	The date picker could partially obscure security prompts. This could be used by a malicious site to trick a user into granting permissions. This vulnerability affects Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14. **CVE ID: CVE-2024-7529**	https://www.mozilla.org/security/advisories/mfsa2024-33/, https://www.mozilla.org/security/advisories/mfsa2024-34/, https://www.mozilla.org/security/advisories/mfsa2024-35/, https://www.mozilla.org/security/advisories/mfsa2024-37/	A-MOZ-THUN-080824/1104
Vendor: Msweet					
Product: pdfio					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.3.1					
Loop with Unreachable Exit Condition ('Infinite Loop')	06-Aug-2024	5.5	PDFio is a simple C library for reading and writing PDF files. There is a denial of service (DOS) vulnerability in the TTF parser. Maliciously crafted TTF files can cause the program to utilize 100% of the Memory and enter an infinite loop. This can also lead to a heap-buffer-overflow vulnerability. An infinite loop occurs in the read_camp function by nGroups value. The ttf.h library is vulnerable. A value called nGroups is extracted from the file, and by changing that value, you can cause the program to utilize 100% of the Memory and enter an infinite loop. If the value of nGroups in the file is small, an infinite loop will not occur. This library, whether used as a standalone binary or as part of another application, is vulnerable to DOS	https://github.com/michaelrsweet/pdfio/commit/e4e1c39578279386b0ab9f9ac14b20a8bad4f935, https://github.com/michaelrsweet/pdfio/security/advisories/GHSA-4hh9-j68x-8353	A-MSW-PDFI-080824/1105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks when parsing certain types of files. Automated systems, including web servers that use this code to convert PDF submissions into plaintext, can be DOSed if an attacker uploads a malicious TTF file. This issue has been addressed in release version 1.3.1. All users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2024-42358**		
Vendor: Nagios					
Product: ndoutils					
Affected Version(s): * Up to (excluding) 2.1.4					
Incorrect Permission Assignment for Critical Resource	07-Aug-2024	7.8	Nagios NDOUtils before 2.1.4 allows privilege escalation from nagios to root because certain executable files are owned by the nagios user. **CVE ID: CVE-2024-43199**	https://github.com/NagiosEnterprises/ndoutils/commit/18ef12037f4a68772d6840cbaa08aa2da07d2891, https://github.com/NagiosEnterprises/ndoutils/pull/65	A-NAG-NDOU-080824/1106
Vendor: ofono_project					
Product: ofono					
Affected Version(s): 2.3					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Aug-2024	7.8	oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability. This vulnerability allows local attackers to execute arbitrary code on affected installations of oFono. An attacker must first obtain the ability to execute code on the target modem in order to exploit this vulnerability. The specific flaw exists within the parsing of STK command PDUs. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-23456. **CVE ID: CVE-2024-7543**	N/A	A-OFO-OFON-080824/1107

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Aug-2024	7.8	oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability. This vulnerability allows local attackers to execute arbitrary code on affected installations of oFono. An attacker must first obtain the ability to execute code on the target modem in order to exploit this vulnerability. The specific flaw exists within the parsing of STK command PDUs. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-23457. **CVE ID: CVE-2024-7544**	N/A	A-OFO-OFON-080824/1108

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Aug-2024	7.8	oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability. This vulnerability allows local attackers to execute arbitrary code on affected installations of oFono. An attacker must first obtain the ability to execute code on the target modem in order to exploit this vulnerability. The specific flaw exists within the parsing of STK command PDUs. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-23458. **CVE ID: CVE-2024-7545**	N/A	A-OFO-OFON-080824/1109

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Aug-2024	7.8	oFono SMS Decoder Stack-based Buffer Overflow Privilege Escalation Vulnerability. This vulnerability allows local attackers to execute arbitrary code on affected installations of oFono. An attacker must first obtain the ability to execute code on the target modem in order to exploit this vulnerability. The specific flaw exists within the parsing of SMS PDUs. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-23460. **CVE ID: CVE-2024-7547**	N/A	A-OFO-OFON-080824/1110
Vendor: online_railway_reservation_system_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: online_railway_reservation_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Aug-2024	4.8	A vulnerability, which was classified as problematic, was found in CodeAstro Online Railway Reservation System 1.0. Affected is an unknown function of the file /admin/admin-add-employee.php of the component Add Employee Page. The manipulation of the argument emp_fname /emp_lname /emp_nat_idno/emp_addr leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7814**	N/A	A-ONL-ONLI-080824/1111
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Aug-2024	4.8	A vulnerability has been found in CodeAstro Online Railway Reservation System 1.0 and classified as problematic. Affected by this vulnerability is an unknown	N/A	A-ONL-ONLI-080824/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functionality of the file /admin/admin-update-employee.php of the component Update Employee Page. The manipulation of the argument emp_fname /emp_lname /emp_nat_idno/emp_addr leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7815**		
Vendor: openeclass					
Product: openeclass					
Affected Version(s): * Up to (excluding) 3.16					
Unrestricted Upload of File with Dangerous Type	12-Aug-2024	9.8	The Open eClass platform (formerly known as GUnet eClass) is a complete Course Management System. An arbitrary file upload vulnerability in the "save" functionality of the H5P module enables unauthenticated users to upload arbitrary files on the server's	https://github.com/gunet/openeclass/commit/4449cf8bed40fd8fc4b267a5726fab9f9fe5a191, https://github.com/gunet/openeclass/security/advisories/GHSA-88c3-hp7p-grgg	A-OPE-OPEN-080824/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filesystem. This may lead in unrestricted RCE on the backend server, since the upload location is accessible from the internet. This vulnerability is fixed in 3.16. **CVE ID: CVE-2024-38530**		
Vendor: Opentext					
Product: arcsight_intelligence					
Affected Version(s): * Up to (excluding) 6.4.13					
N/A	06-Aug-2024	9.8	Privilege escalation vulnerability identified in OpenText ArcSight Intelligence. **CVE ID: CVE-2024-6359**	https://portal.microfocus.com/s/article/KM000032594	A-OPE-ARCS-080824/1114
Authorization Bypass Through User-Controlled Key	06-Aug-2024	8.8	Insecure Direct Object Reference vulnerability identified in OpenText ArcSight Intelligence. **CVE ID: CVE-2024-6357**	N/A	A-OPE-ARCS-080824/1115
Incorrect Authorization	06-Aug-2024	8.8	Incorrect Authorization vulnerability identified in OpenText ArcSight Intelligence. **CVE ID: CVE-2024-6358**	N/A	A-OPE-ARCS-080824/1116
Product: directory_services					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.4.2 Up to (excluding) 24.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	9.8	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in OpenText OpenText Directory Services allows Path Traversal.This issue affects OpenText Directory Services: from 16.4.2 before 24.1. **CVE ID: CVE-2023-7249**	N/A	A-OPE-DIRE-080824/1117
Vendor: openwebui					
Product: open_webui					
Affected Version(s): 0.1.105					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Aug-2024	8.8	Attacker controlled files can be uploaded to arbitrary locations on the web server's filesystem by abusing a path traversal vulnerability. **CVE ID: CVE-2024-6707**	N/A	A-OPE-OPEN-080824/1118
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2024	6.1	Attackers can craft a malicious prompt that coerces the language model into executing arbitrary JavaScript in the context of the web page.	N/A	A-OPE-OPEN-080824/1119

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-6706		
Vendor: oretnom23					
Product: car_driving_school_management_system					
Affected Version(s): 1.0					
Cross-Site Request Forgery (CSRF)	12-Aug-2024	8.8	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been classified as problematic. This affects the function save_users of the file admin/user/index.php. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7661**	N/A	A-ORE-CAR_-080824/1120
Cross-Site Request Forgery (CSRF)	12-Aug-2024	6.5	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been declared as problematic. This vulnerability affects the function save_package of the file	N/A	A-ORE-CAR_-080824/1121

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin/packages/manag_package.php. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7662**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	6.1	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been declared as problematic. Affected by this vulnerability is the function update_settings_info of the file /classes/SystemSettings.php?f=update_settings. The manipulation of the argument contact/address leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7677**	N/A	A-ORE-CAR_-080824/1122

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	6.1	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /classes/Master.php?f=save_package. The manipulation of the argument name/description/training_duration leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7678**	N/A	A-ORE-CAR_-080824/1123
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	5.3	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file manage_user.php. The manipulation	N/A	A-ORE-CAR_-080824/1124

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7663**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	5.3	A vulnerability, which was classified as critical, has been found in SourceCodester Car Driving School Management System 1.0. Affected by this issue is some unknown functionality of the file view_package.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7666**	N/A	A-ORE-CAR_-080824/1125
Improper Neutralization of Special Elements used in an	12-Aug-2024	5.3	A vulnerability, which was classified as critical, was found in SourceCodester Car Driving School	N/A	A-ORE-CAR_-080824/1126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			Management System 1.0. This affects the function delete_users of the file User.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7667**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	5.3	A vulnerability has been found in SourceCodester Car Driving School Management System 1.0 and classified as critical. This vulnerability affects the function delete_package of the file Master.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7668**	N/A	A-ORE-CAR_-080824/1127
Improper Neutralization of	12-Aug-2024	5.3	A vulnerability was found in SourceCodester Car	N/A	A-ORE-CAR_-080824/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			Driving School Management System 1.0 and classified as critical. This issue affects the function delete_enrollment of the file Master.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7669**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	5.3	A vulnerability was found in Sourcecodester Car Driving School Management System 1.0. It has been classified as critical. Affected is the function save_package of the file /classes/Master.php?f=save_package. 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	N/A	A-ORE-CAR_-080824/1129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. **CVE ID: CVE-2024-7676**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	4.3	A vulnerability classified as critical has been found in SourceCodester Car Driving School Management System 1.0. Affected is an unknown function of the file view_details.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. **CVE ID: CVE-2024-7664**	N/A	A-ORE-CAR_-080824/1130
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	4.3	A vulnerability classified as critical was found in SourceCodester Car Driving School Management System 1.0. Affected by this vulnerability is an unknown functionality of the file manage_package.php. The manipulation of the	N/A	A-ORE-CAR_-080824/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7665**		
Product: clinics_patient_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Aug-2024	7.5	A vulnerability classified as critical was found in SourceCodester Clinics Patient Management System 1.0. This vulnerability affects unknown code of the file /pms/ajax/check_user_name.php. The manipulation of the argument user_name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7841**	N/A	A-ORE-CLIN-080824/1132
Product: clinic\'s_patient_management_system					
Affected Version(s): 1.0					
Improper Neutralization of	05-Aug-2024	9.8	A vulnerability, which was classified as critical,	N/A	A-ORE-CLIN-080824/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			has been found in SourceCodester Clinics Patient Management System 1.0. Affected by this issue is some unknown functionality of the file /new_prescription.php. The manipulation of the argument patient leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273620. **CVE ID: CVE-2024-7494**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Aug-2024	7.5	A vulnerability has been found in SourceCodester Clinics Patient Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /medicines.php. The manipulation of the argument medicine_name	N/A	A-ORE-CLIN-080824/1134

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7750**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Aug-2024	7.5	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /update_medicine.php. The manipulation of the argument hidden_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7751**	N/A	A-ORE-CLIN-080824/1135
Direct Request ('Forced Browsing')	14-Aug-2024	7.5	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been declared as	N/A	A-ORE-CLIN-080824/1136

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problematic. This vulnerability affects unknown code of the file /user_images/. The manipulation leads to direct request. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7753**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Aug-2024	7.5	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /ajax/check_medicine_name.php. The manipulation of the argument user_name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7754**	N/A	A-ORE-CLIN-080824/1137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	6.1	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /update_medicine.php. The manipulation of the argument medicine_name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7752**	N/A	A-ORE-CLIN-080824/1138
Cross-Site Request Forgery (CSRF)	12-Aug-2024	5.4	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file users.php of the component User Page. The manipulation leads to cross-site request forgery.	N/A	A-ORE-CLIN-080824/1139

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7645**		
Product: computer_laboratory_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2024	9.8	SourceCodester Computer Laboratory Management System 1.0 allows classes/Master.php id SQL Injection. **CVE ID: CVE-2024-34479**	N/A	A-ORE-COMP-080824/1140
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2024	9.8	SourceCodester Computer Laboratory Management System 1.0 allows admin/category/view_category.php id SQL Injection. **CVE ID: CVE-2024-34480**	N/A	A-ORE-COMP-080824/1141
N/A	12-Aug-2024	6.5	Incorrect access control in the delete_category function of Sourcecodester Computer Laboratory Management System v1.0 allows authenticated attackers with low-level privileges to	N/A	A-ORE-COMP-080824/1142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrarily delete categories. **CVE ID: CVE-2024-41332**		
Product: simple_online_bidding_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Aug-2024	9.8	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been classified as critical. Affected is an unknown function of the file /simple-online-bidding-system/bidding/admin/ajax.php?action=login. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7797**	N/A	A-ORE-SIMP-080824/1143
Improper Neutralization of Special Elements used in an SQL Command	15-Aug-2024	9.8	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been declared as critical. Affected by this vulnerability is an	N/A	A-ORE-SIMP-080824/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			unknown functionality of the file /simple-online-bidding-system/bidding/admin/ajax.php?action=login2. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7798**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Aug-2024	7.5	A vulnerability classified as critical has been found in SourceCodester Simple Online Bidding System 1.0. This affects an unknown part of the file /simple-online-bidding-system/bidding/admin/ajax.php?action=delete_product. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	N/A	A-ORE-SIMP-080824/1145

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7800		
N/A	15-Aug-2024	7.3	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /simple-online-bidding-system/bidding/admin/users.php. The manipulation leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7799**	N/A	A-ORE-SIMP-080824/1146
Product: simple_realtime_quiz_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Aug-2024	9.8	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0 and classified as critical. This issue affects some unknown processing of the file /ajax.php?action=login of the	N/A	A-ORE-SIMP-080824/1147

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component Login. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273353 was assigned to this vulnerability. **CVE ID: CVE-2024-7369**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2024	9.8	A vulnerability classified as critical was found in SourceCodester Simple Realtime Quiz System 1.0. This vulnerability affects unknown code of the file /manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273358 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-7374**	N/A	A-ORE-SIMP-080824/1148

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Simple Realtime Quiz System 1.0. This issue affects some unknown processing of the file /my_quiz_result.php. The manipulation of the argument quiz leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273359. **CVE ID: CVE-2024-7375**	N/A	A-ORE-SIMP-080824/1149
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Simple Realtime Quiz System 1.0. Affected is an unknown function of the file /print_quiz_records.php. The manipulation of the argument id leads	N/A	A-ORE-SIMP-080824/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-273360. **CVE ID: CVE-2024-7376**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2024	9.8	A vulnerability has been found in SourceCodester Simple Realtime Quiz System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /view_result.php. The manipulation of the argument qid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273361 was assigned to this vulnerability. **CVE ID: CVE-2024-7377**	N/A	A-ORE-SIMP-080824/1151
Improper Neutralization of	02-Aug-2024	9.8	A vulnerability was found in SourceCodester	N/A	A-ORE-SIMP-080824/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			Simple Realtime Quiz System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /manage_question.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-273362 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-7378**		
Cross-Site Request Forgery (CSRF)	01-Aug-2024	8.8	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Realtime Quiz System 1.0. This affects an unknown part of the file /ajax.php?action=save_user. The manipulation leads to cross-site request forgery. It is possible to initiate the attack	N/A	A-ORE-SIMP-080824/1153

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273351. **CVE ID: CVE-2024-7367**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Aug-2024	8.8	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0. It has been classified as critical. Affected is an unknown function of the file /manage_quiz.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. VDB-273354 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-7370**	N/A	A-ORE-SIMP-080824/1154
Improper Neutralization of Special Elements used in an	01-Aug-2024	8.8	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0. It has been declared	N/A	A-ORE-SIMP-080824/1155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			as critical. Affected by this vulnerability is an unknown functionality of the file /quiz_view.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273355. **CVE ID: CVE-2024-7371**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2024	8.8	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /quiz_board.php. The manipulation of the argument quiz leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may	N/A	A-ORE-SIMP-080824/1156

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. The identifier of this vulnerability is VDB-273356. **CVE ID: CVE-2024-7372**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2024	8.8	A vulnerability classified as critical has been found in SourceCodester Simple Realtime Quiz System 1.0. This affects an unknown part of the file /ajax.php?action=load_answered. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273357 was assigned to this vulnerability. **CVE ID: CVE-2024-7373**	N/A	A-ORE-SIMP-080824/1157
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2024	5.4	A vulnerability has been found in SourceCodester Simple Realtime Quiz System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /ajax.php?action=s	N/A	A-ORE-SIMP-080824/1158

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ave_quiz. The manipulation of the argument title leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273352. **CVE ID: CVE-2024-7368**		
Product: tracking_monitoring_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Aug-2024	9.8	A vulnerability classified as critical was found in SourceCodester Tracking Monitoring Management System 1.0. This vulnerability affects unknown code of the file /ajax.php?action=save_establishment. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this	N/A	A-ORE-TRAC-080824/1159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-273340. **CVE ID: CVE-2024-7361**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Tracking Monitoring Management System 1.0. This issue affects some unknown processing of the file /manage_user.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273341 was assigned to this vulnerability. **CVE ID: CVE-2024-7362**	N/A	A-ORE-TRAC-080824/1160
Improper Neutralization of Special Elements used in an SQL Command	01-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Tracking Monitoring Management System 1.0.	N/A	A-ORE-TRAC-080824/1161

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			Affected is an unknown function of the file /manage_person.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. VDB-273342 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-7363**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Aug-2024	9.8	A vulnerability has been found in SourceCodester Tracking Monitoring Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /manage_records.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may	N/A	A-ORE-TRAC-080824/1162

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. The associated identifier of this vulnerability is VDB-273343. **CVE ID: CVE-2024-7364**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Aug-2024	9.8	A vulnerability was found in SourceCodester Tracking Monitoring Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /manage_establishment.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273344. **CVE ID: CVE-2024-7365**	N/A	A-ORE-TRAC-080824/1163
Improper Neutralization of Special Elements used in an SQL	01-Aug-2024	9.8	A vulnerability was found in SourceCodester Tracking Monitoring Management System 1.0. It has	N/A	A-ORE-TRAC-080824/1164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			been classified as critical. This affects an unknown part of the file /ajax.php?action=login of the component Login. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273345 was assigned to this vulnerability. **CVE ID: CVE-2024-7366**		
Cross-Site Request Forgery (CSRF)	01-Aug-2024	8.8	A vulnerability classified as problematic has been found in SourceCodester Tracking Monitoring Management System 1.0. This affects an unknown part of the file /ajax.php. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the	N/A	A-ORE-TRAC-080824/1165

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. The associated identifier of this vulnerability is VDB-273339. **CVE ID: CVE-2024-7360**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2024	6.1	A vulnerability was found in SourceCodester Tracking Monitoring Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /ajax.php?action=save_establishment. The manipulation of the argument name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-273338 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-7359**	N/A	A-ORE-TRAC-080824/1166
Vendor: Paloaltonetworks					
Product: cortex_xsoar_commonscripts					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.12.33					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Aug-2024	9.8	A command injection issue in Palo Alto Networks Cortex XSOAR CommonScripts Pack allows an unauthenticated attacker to execute arbitrary commands within the context of an integration container. **CVE ID: CVE-2024-5914**	https://security.paloaltonetworks.com/CVE-2024-5914	A-PAL-CORT-080824/1167
Product: globalprotect					
Affected Version(s): 6.3.0					
Incorrect Permission Assignment for Critical Resource	14-Aug-2024	7.8	A privilege escalation (PE) vulnerability in the Palo Alto Networks GlobalProtect app on Windows devices enables a local user to execute programs with elevated privileges. **CVE ID: CVE-2024-5915**	https://security.paloaltonetworks.com/CVE-2024-5915	A-PAL-GLOB-080824/1168
Affected Version(s): From (including) 5.1.0 Up to (including) 5.1.9					
Incorrect Permission Assignment for Critical Resource	14-Aug-2024	7.8	A privilege escalation (PE) vulnerability in the Palo Alto Networks GlobalProtect app on Windows devices enables a local user to execute programs	https://security.paloaltonetworks.com/CVE-2024-5915	A-PAL-GLOB-080824/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with elevated privileges. **CVE ID: CVE-2024-5915**		
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.6					
Incorrect Permission Assignment for Critical Resource	14-Aug-2024	7.8	A privilege escalation (PE) vulnerability in the Palo Alto Networks GlobalProtect app on Windows devices enables a local user to execute programs with elevated privileges. **CVE ID: CVE-2024-5915**	https://security.paloaltonetworks.com/CVE-2024-5915	A-PAL-GLOB-080824/1170
Affected Version(s): From (including) 6.1.0 Up to (excluding) 6.1.5					
Incorrect Permission Assignment for Critical Resource	14-Aug-2024	7.8	A privilege escalation (PE) vulnerability in the Palo Alto Networks GlobalProtect app on Windows devices enables a local user to execute programs with elevated privileges. **CVE ID: CVE-2024-5915**	https://security.paloaltonetworks.com/CVE-2024-5915	A-PAL-GLOB-080824/1171
Affected Version(s): From (including) 6.2.0 Up to (excluding) 6.2.4					
Incorrect Permission Assignment for Critical Resource	14-Aug-2024	7.8	A privilege escalation (PE) vulnerability in the Palo Alto Networks GlobalProtect app on Windows devices enables a local user to	https://security.paloaltonetworks.com/CVE-2024-5915	A-PAL-GLOB-080824/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute programs with elevated privileges. **CVE ID: CVE-2024-5915**		
Vendor: phpgurukul					
Product: old_age_home_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	6.1	A Reflected Cross Site Scripting (XSS) vulnerability was found in "/oahms/search.php" in PHPGurukul Old Age Home Management System v1.0, which allows remote attackers to execute arbitrary code via the "searchdata" parameter. **CVE ID: CVE-2024-40484**	N/A	A-PHP-OLD_-080824/1173
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	5.4	A Stored Cross Site Scripting (XSS) vulnerability was found in "/admin/view-enquiry.php" in PHPGurukul Old Age Home Management System v1.0, which allows remote attackers to execute arbitrary code via the Contact Us page	N/A	A-PHP-OLD_-080824/1174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"message" parameter. **CVE ID: CVE-2024-40481**		
Product: tourism_management_system					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in Phpgurukul Tourism Management System v2.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload into the uname parameter. **CVE ID: CVE-2024-41333**	N/A	A-PHP-TOUR-080824/1175
Vendor: pmweb					
Product: pmweb					
Affected Version(s): 7.2.00					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2024	5.4	A vulnerability has been found in PMWeb 7.2.00 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Web Application Firewall. The manipulation leads to cross site scripting. The	N/A	A-PMW-PMWE-080824/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273559. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7466**		
Vendor: Postgresql					
Product: postgresql					
Affected Version(s): From (including) 12.0 Up to (excluding) 12.20					
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2024	7.5	Time-of-check Time-of-use (TOCTOU) race condition in pg_dump in PostgreSQL allows an object creator to execute arbitrary SQL functions as the user running pg_dump, which is often a superuser. The attack involves replacing another relation type with a view or foreign table. The attack requires waiting for pg_dump to start, but winning the race condition	https://www.postgresql.org/support/security/CVE-2024-7348/	A-POS-POST-080824/1177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is trivial if the attacker retains an open transaction. Versions before PostgreSQL 16.4, 15.8, 14.13, 13.16, and 12.20 are affected. **CVE ID: CVE-2024-7348**		
Affected Version(s): From (including) 13.0 Up to (excluding) 13.16					
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2024	7.5	Time-of-check Time-of-use (TOCTOU) race condition in pg_dump in PostgreSQL allows an object creator to execute arbitrary SQL functions as the user running pg_dump, which is often a superuser. The attack involves replacing another relation type with a view or foreign table. The attack requires waiting for pg_dump to start, but winning the race condition is trivial if the attacker retains an open transaction. Versions before PostgreSQL 16.4, 15.8, 14.13, 13.16, and 12.20 are affected. **CVE ID: CVE-2024-7348**	https://www.postgresql.org/support/security/CVE-2024-7348/	A-POS-POST-080824/1178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 14.0 Up to (excluding) 14.13					
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2024	7.5	Time-of-check Time-of-use (TOCTOU) race condition in pg_dump in PostgreSQL allows an object creator to execute arbitrary SQL functions as the user running pg_dump, which is often a superuser. The attack involves replacing another relation type with a view or foreign table. The attack requires waiting for pg_dump to start, but winning the race condition is trivial if the attacker retains an open transaction. Versions before PostgreSQL 16.4, 15.8, 14.13, 13.16, and 12.20 are affected. **CVE ID: CVE-2024-7348**	https://www.postgresql.org/support/security/CVE-2024-7348/	A-POS-POST-080824/1179
Affected Version(s): From (including) 15.0 Up to (excluding) 15.8					
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2024	7.5	Time-of-check Time-of-use (TOCTOU) race condition in pg_dump in PostgreSQL allows an object creator to execute arbitrary SQL functions as the user running	https://www.postgresql.org/support/security/CVE-2024-7348/	A-POS-POST-080824/1180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pg_dump, which is often a superuser. The attack involves replacing another relation type with a view or foreign table. The attack requires waiting for pg_dump to start, but winning the race condition is trivial if the attacker retains an open transaction. Versions before PostgreSQL 16.4, 15.8, 14.13, 13.16, and 12.20 are affected. **CVE ID: CVE-2024-7348**		
Affected Version(s): From (including) 16.0 Up to (excluding) 16.4					
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2024	7.5	Time-of-check Time-of-use (TOCTOU) race condition in pg_dump in PostgreSQL allows an object creator to execute arbitrary SQL functions as the user running pg_dump, which is often a superuser. The attack involves replacing another relation type with a view or foreign table. The attack requires waiting for pg_dump to start, but winning the race condition	https://www.postgresql.org/support/security/CVE-2024-7348/	A-POS-POST-080824/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is trivial if the attacker retains an open transaction. Versions before PostgreSQL 16.4, 15.8, 14.13, 13.16, and 12.20 are affected. **CVE ID: CVE-2024-7348**		
Vendor: prison_management_system_project					
Product: prison_management_system					
Affected Version(s): 1.0					
Insufficiently Protected Credentials	15-Aug-2024	7.5	A vulnerability, which was classified as problematic, has been found in SourceCodester Prison Management System 1.0. This issue affects some unknown processing of the file /uploadImage/Profile/ of the component Profile Image Handler. The manipulation leads to insufficiently protected credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7813**	N/A	A-PRI-PRIS-080824/1182

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Projectsend					
Product: projectsend					
Affected Version(s): * Up to (excluding) r1720					
Use of Insufficiently Random Values	12-Aug-2024	7.5	A vulnerability, which was classified as problematic, was found in projectsend up to r1605. Affected is the function generate_random_string of the file includes/functions.php of the component Password Reset Token Handler. The manipulation leads to insufficiently random values. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. Upgrading to version r1720 is able to address this issue. The name of the patch is aa27eb97edc2ff2b203f97e6675d7b5ba0a22a17. It is recommended to upgrade the affected component.	https://github.com/projectsend/projectsend/commit/aa27eb97edc2ff2b203f97e6675d7b5ba0a22a17	A-PRO-PROJ-080824/1183

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7659		
Authorization Bypass Through User-Controlled Key	12-Aug-2024	5.3	A vulnerability, which was classified as problematic, has been found in projectsend up to r1605. This issue affects the function get_preview of the file process.php. The manipulation leads to improper control of resource identifiers. The attack may be initiated remotely. Upgrading to version r1720 is able to address this issue. The patch is named eb5a04774927e5855b9d0e5870a2aae5a3dc5a08. It is recommended to upgrade the affected component. **CVE ID: CVE-2024-7658**	https://github.com/projectsend/projectsend/commit/eb5a04774927e5855b9d0e5870a2aae5a3dc5a08	A-PRO-PROJ-080824/1184
Vendor: projectworlds					
Product: online_examination_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL	15-Aug-2024	9.8	Projectworlds Online Examination System v1.0 is vulnerable to SQL Injection via the subject parameter in feed.php.	N/A	A-PRO-ONLI-080824/1185

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			**CVE ID: CVE-2024-42843**		
Vendor: pylonsproject					
Product: webob					
Affected Version(s): * Up to (excluding) 1.8.8					
URL Redirection to Untrusted Site ('Open Redirect')	14-Aug-2024	6.1	WebOb provides objects for HTTP requests and responses. When WebOb normalizes the HTTP Location header to include the request hostname, it does so by parsing the URL that the user is to be redirected to with Python's urlparse, and joining it to the base URL. `urlparse` however treats a `//` at the start of a string as a URI without a scheme, and then treats the next part as the hostname. `urljoin` will then use that hostname from the second part as the hostname replacing the original one from the request. This vulnerability is patched in WebOb version 1.8.8. **CVE ID: CVE-2024-42353**	https://github.com/Pylons/webob/commit/f689bcf4f0a1f64f1735b1d5069aef5be6974b5b, https://github.com/Pylons/webob/security/advisories/GHSA-mg3v-6m49-jhp3	A-PYL-WEBO-080824/1186
Vendor: qwik					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qwik					
Affected Version(s): * Up to (excluding) 1.7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	Qwik is a performance focused javascript framework. A potential mutation XSS vulnerability exists in Qwik for versions up to but not including 1.6.0. Qwik improperly escapes HTML on server-side rendering. It converts strings according to the rules found in the `render-ssr.ts` file. It sometimes causes the situation that the final DOM tree rendered on browsers is different from what Qwik expects on server-side rendering. This may be leveraged to perform XSS attacks, and a type of the XSS is known as mXSS (mutation XSS). This has been resolved in qwik version 1.6.0 and @builder.io/qwik version 1.7.3. All users are advised to upgrade. There are no known workarounds for this vulnerability.	https://github.com/QwikDev/qwik/commit/7e742eb3a1001542d795776c0317d47df8b9d64e, https://github.com/QwikDev/qwik/security/advisories/GHSA-2rwj-7xq8-4gx4	A-QWI-QWIK-080824/1187

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41677		
Vendor: Redhat					
Product: openshift_ai					
Affected Version(s): -					
N/A	12-Aug-2024	8.8	A vulnerability was found in OpenShift AI that allows for authentication bypass and privilege escalation across models within the same namespace. When deploying AI models, the UI provides the option to protect models with authentication. However, credentials from one model can be used to access other models and APIs within the same namespace. The exposed ServiceAccount tokens, visible in the UI, can be utilized with oc --token={token} to exploit the elevated view privileges associated with the ServiceAccount, leading to unauthorized access to additional resources.	https://access.redhat.com/security/cve/CVE-2024-7557	A-RED-OPEN-080824/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7557		
Product: openshift_data_science					
Affected Version(s): -					
N/A	12-Aug-2024	8.8	A vulnerability was found in OpenShift AI that allows for authentication bypass and privilege escalation across models within the same namespace. When deploying AI models, the UI provides the option to protect models with authentication. However, credentials from one model can be used to access other models and APIs within the same namespace. The exposed ServiceAccount tokens, visible in the UI, can be utilized with oc --token={token} to exploit the elevated view privileges associated with the ServiceAccount, leading to unauthorized access to additional resources. **CVE ID: CVE-2024-7557**	https://access.redhat.com/security/cve/CVE-2024-7557	A-RED-OPEN-080824/1189

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: rems					
Product: accounts_manager_app					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Accounts Manager App 1.0. This issue affects some unknown processing of the file /endpoint/delete-account.php. The manipulation of the argument account leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7748**	N/A	A-REM-ACCO-080824/1190
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Aug-2024	5.4	A vulnerability, which was classified as problematic, was found in SourceCodester Accounts Manager App 1.0. Affected is an unknown function of the file /endpoint/add-account.php. The manipulation of the argument	N/A	A-REM-ACCO-080824/1191

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account_name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7749**		
Product: daily_calories_monitoring_tool					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	9.8	Sourcecodester Daily Calories Monitoring Tool v1.0 is vulnerable to SQL Injection via "delete-calorie.php." **CVE ID: CVE-2024-40472**	N/A	A-REM-DAIL-080824/1192
Product: daily_expenses_monitoring_app					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Aug-2024	9.8	A vulnerability classified as critical has been found in SourceCodester Daily Expenses Monitoring App 1.0. This affects an unknown part of the file /endpoint/delete-expense.php. The manipulation of the argument expense leads to sql injection. It is possible to initiate	N/A	A-REM-DAIL-080824/1193

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7811**		
Product: file_manager_app					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	6.1	A vulnerability has been found in SourceCodester File Manager App 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Add File Handler. The manipulation of the argument File Title/Uploaded By leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7660**	N/A	A-REM-FILE-080824/1194
Product: leads_manager_tool					
Affected Version(s): 1.0					
Improper Neutralization of Special	12-Aug-2024	9.8	A vulnerability was found in SourceCodester Leads Manager	N/A	A-REM-LEAD-080824/1195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			Tool 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /endpoint/delete-leads.php of the component Delete Leads Handler. The manipulation of the argument leads leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7643**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	5.4	A vulnerability was found in SourceCodester Leads Manager Tool 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/add-leads.php of the component Add Leads Handler. The manipulation of the argument leads_name/phone_number leads to cross site scripting. It is possible to initiate the attack	N/A	A-REM-LEAD-080824/1196

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7644**		
Product: task_progress_tracker					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Aug-2024	8.8	A vulnerability was found in SourceCodester Task Progress Tracker 1.0. It has been classified as critical. Affected is an unknown function of the file /endpoint/delete-task.php. The manipulation of the argument task leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7792**	N/A	A-REM-TASK-080824/1197
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-2024	5.4	A vulnerability was found in SourceCodester Task Progress Tracker 1.0. It has been declared as problematic. Affected by this vulnerability is an	N/A	A-REM-TASK-080824/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unknown functionality of the file /endpoint/add-task.php. The manipulation of the argument task_name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7793**		
Vendor: Samsung					
Product: magicinfo_9_server					
Affected Version(s): * Up to (excluding) 21.1050					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	Improper limitation of a pathname to a restricted directory vulnerability in Samsung MagicINFO 9 Server version before 21.1050 allows attackers to write arbitrary file as system authority. **CVE ID: CVE-2024-7399**	https://security.samsungtv.com/securityUpdates	A-SAM-MAGI-080824/1199
Product: notes					
Affected Version(s): * Up to (excluding) 4.4.21.62					
Out-of-bounds Write	07-Aug-2024	7.8	Out-of-bounds write in appending paragraph in Samsung Notes prior to version	https://security.samsungmobile.com/serviceWe	A-SAM-NOTE-080824/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.4.21.62 allows local attackers to potentially execute arbitrary code with Samsung Notes privilege. **CVE ID: CVE-2024-34622**	b.smsb?year=2024&month=08	
Out-of-bounds Write	07-Aug-2024	7.8	Out-of-bounds write in applying connected information in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially execute arbitrary code with Samsung Notes privilege. **CVE ID: CVE-2024-34623**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1201
Out-of-bounds Read	07-Aug-2024	5.5	Out-of-bounds read in applying binary with data in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory. **CVE ID: CVE-2024-34621**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1202
Out-of-bounds Read	07-Aug-2024	5.5	Out-of-bounds read in applying paragraphs in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory.	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1203

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-34624		
Out-of-bounds Read	07-Aug-2024	5.5	Out-of-bounds read in applying connection point in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory. **CVE ID: CVE-2024-34625**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1204
Out-of-bounds Read	07-Aug-2024	5.5	Out-of-bounds read in applying own binary in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory. **CVE ID: CVE-2024-34626**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1205
Out-of-bounds Read	07-Aug-2024	5.5	Out-of-bounds read in parsing implemention in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory. **CVE ID: CVE-2024-34627**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1206
Out-of-bounds Read	07-Aug-2024	5.5	Out-of-bounds read in applying binary with path in Samsung Notes prior to version 4.4.21.62 allows local attackers to	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1207

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially read memory. **CVE ID: CVE-2024-34628**		
Out-of-bounds Read	07-Aug-2024	5.5	Out-of-bounds read in applying binary with text common object in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory. **CVE ID: CVE-2024-34629**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1208
Out-of-bounds Read	07-Aug-2024	5.5	Out-of-bounds read in applying own binary with textbox in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory. **CVE ID: CVE-2024-34630**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1209
Out-of-bounds Read	07-Aug-2024	5.5	Out-of-bounds read in applying new binary in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory. **CVE ID: CVE-2024-34631**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1210
Out-of-bounds Read	07-Aug-2024	3.3	Out-of-bounds read in parsing object header in Samsung	https://security.samsungmobile.com/serviceWe	A-SAM-NOTE-080824/1211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Notes prior to version 4.4.21.62 allows local attacker to access unauthorized memory. **CVE ID: CVE-2024-34633**	b.smsb?year=2024&month=08	
Out-of-bounds Read	07-Aug-2024	3.3	Out-of-bounds read in parsing connected object list in Samsung Notes prior to version 4.4.21.62 allows local attacker to access unauthorized memory. **CVE ID: CVE-2024-34634**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1212
Out-of-bounds Read	07-Aug-2024	3.3	Out-of-bounds read in parsing textbox object in Samsung Notes prior to version 4.4.21.62 allows local attacker to access unauthorized memory. **CVE ID: CVE-2024-34635**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1213
Affected Version(s): * Up to (including) 4.4.21.62					
Out-of-bounds Read	07-Aug-2024	3.3	Out-of-bounds read in uuid parsing in Samsung Notes prior to version 4.4.21.62 allows local attacker to access unauthorized memory.	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=08	A-SAM-NOTE-080824/1214

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-34632		
Vendor: scilico					
Product: i-librarian					
Affected Version(s): * Up to (including) 5.11.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	8.6	Cross Site Scripting vulnerability in Martin Kucej i-librarian v.5.11.0 and before allows a local attacker to execute arbitrary code via the search function in the import component. **CVE ID: CVE-2024-40500**	N/A	A-SCI-I-LI-080824/1215
Vendor: Shopware					
Product: shopware					
Affected Version(s): * Up to (excluding) 6.5.8.13					
Improper Control of Generation of Code ('Code Injection')	08-Aug-2024	9.8	Shopware, an open ecommerce platform, has a new Twig Tag `sw_silent_feature_call` which silences deprecation messages while triggered in this tag. Prior to versions 6.6.5.1 and 6.5.8.13, it accepts as parameter a string the feature flag name to silence, but this parameter is not escaped properly and allows execution of code. Update to	https://github.com/shopware/core/commit/a784aa1cec0624e36e0ee4d41aeebaed40e0442f, https://github.com/shopware/core/commit/d35ee2eda5c995faeb08b3dad127eab65c64e2a2, https://github.com/shopware/shopware/commit/445c6763cc093fbd651e0efaa4150deae4ae60da	A-SHO-SHOP-080824/1216

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Shopware 6.6.5.1 or 6.5.8.13 to receive a patch. For older versions of 6.2, 6.3, and 6.4, corresponding security measures are also available via a plugin. **CVE ID: CVE-2024-42355**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2024	9.8	Shopware is an open commerce platform. Prior to versions 6.6.5.1 and 6.5.8.13, the Shopware application API contains a search functionality which enables users to search through information stored within their Shopware instance. The searches performed by this function can be aggregated using the parameters in the `aggregations` object. The `name` field in this `aggregations` object is vulnerable SQL-injection and can be exploited using SQL parameters. Update to Shopware 6.6.5.1 or 6.5.8.13 to receive a patch. For older versions of	https://github.com/shopware/core/commit/63c05615694790f5790a04ef889f42b764fa53c9, https://github.com/shopware/core/commit/a784aa1cec0624e36e0ee4d41aeebaed40e0442f, https://github.com/shopware/shopware/commit/57ea2f3c59483cf7c0f853e7a0d68c23ded1fe5b	A-SHO-SHOP-080824/1217

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.1, 6.2, 6.3, and 6.4, corresponding security measures are also available via a plugin. **CVE ID: CVE-2024-42357**		
Improper Control of Generation of Code ('Code Injection')	08-Aug-2024	7.2	Shopware is an open commerce platform. Prior to versions 6.6.5.1 and 6.5.8.13, the `context` variable is injected into almost any Twig Template and allows to access to current language, currency information. The context object allows also to switch for a short time the scope of the Context as a helper with a callable function. The function can be called also from Twig and as the second parameter allows any callable, it's possible to call from Twig any statically callable PHP function/method. It's not possible as customer to provide any Twig code, the attacker would require access to Administration to	https://github.com/shopware/core/commit/04183e0c02af3b404eb7d52c683734bfe0595038, https://github.com/shopware/core/commit/a784aa1cec0624e36e0ee4d41aeebaed40e0442f, https://github.com/shopware/shopware/commit/8504ba7e56e53add6a1d5b9d45015e3d899cd0ac	A-SHO-SHOP-080824/1218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit it using Mail templates or using App Scripts. Update to Shopware 6.6.5.1 or 6.5.8.13 to receive a patch. For older versions of 6.1, 6.2, 6.3 and 6.4 corresponding security measures are also available via a plugin. **CVE ID: CVE-2024-42356**		
N/A	08-Aug-2024	5.9	Shopware is an open commerce platform. The store-API works with regular entities and not expose all fields for the public API; fields need to be marked as ApiAware in the EntityDefinition. So only ApiAware fields of the EntityDefinition will be encoded to the final JSON. Prior to versions 6.6.5.1 and 6.5.8.13, the processing of the Criteria did not considered ManyToMany associations and so they were not considered properly and the protections didn't get used. This issue	https://github.com/shopware/core/commit/a784aa1cec0624e36e0ee4d41aeebaed40e0442f, https://github.com/shopware/core/commit/d35ee2eda5c995faeb08b3dad127eab65c64e2a2, https://github.com/shopware/shopware/commit/8504ba7e56e53add6a1d5b9d45015e3d899cd0ac	A-SHO-SHOP-080824/1219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cannot be reproduced with the default entities by Shopware, but can be triggered with extensions. Update to Shopware 6.6.5.1 or 6.5.8.13 to receive a patch. For older versions of 6.2, 6.3, and 6.4, corresponding security measures are also available via a plugin. **CVE ID: CVE-2024-42354**		
Affected Version(s): From (including) 6.6.0.0 Up to (excluding) 6.6.5.1					
Improper Control of Generation of Code ('Code Injection')	08-Aug-2024	9.8	Shopware, an open ecommerce platform, has a new Twig Tag `sw_silent_feature_call` which silences deprecation messages while triggered in this tag. Prior to versions 6.6.5.1 and 6.5.8.13, it accepts as parameter a string the feature flag name to silence, but this parameter is not escaped properly and allows execution of code. Update to Shopware 6.6.5.1 or 6.5.8.13 to receive a patch. For	https://github.com/shopware/core/commit/a784aa1cec0624e36e0ee4d41aeebaed40e0442f, https://github.com/shopware/core/commit/d35ee2eda5c995faeb08b3dad127eab65c64e2a2, https://github.com/shopware/shopware/commit/445c6763cc093fbd651e0efaa4150deae4ae60da	A-SHO-SHOP-080824/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			older versions of 6.2, 6.3, and 6.4, corresponding security measures are also available via a plugin. **CVE ID: CVE-2024-42355**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2024	9.8	Shopware is an open commerce platform. Prior to versions 6.6.5.1 and 6.5.8.13, the Shopware application API contains a search functionality which enables users to search through information stored within their Shopware instance. The searches performed by this function can be aggregated using the parameters in the `aggregations` object. The `name` field in this `aggregations` object is vulnerable SQL-injection and can be exploited using SQL parameters. Update to Shopware 6.6.5.1 or 6.5.8.13 to receive a patch. For older versions of 6.1, 6.2, 6.3, and 6.4, corresponding security measures	https://github.com/shopware/core/commit/63c05615694790f5790a04ef889f42b764fa53c9, https://github.com/shopware/core/commit/a784aa1cec0624e36e0ee4d41aeebaed40e0442f, https://github.com/shopware/shopware/commit/57ea2f3c59483cf7c0f853e7a0d68c23ded1fe5b	A-SHO-SHOP-080824/1221

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are also available via a plugin. **CVE ID: CVE-2024-42357**		
Improper Control of Generation of Code ('Code Injection')	08-Aug-2024	7.2	Shopware is an open commerce platform. Prior to versions 6.6.5.1 and 6.5.8.13, the `context` variable is injected into almost any Twig Template and allows to access to current language, currency information. The context object allows also to switch for a short time the scope of the Context as a helper with a callable function. The function can be called also from Twig and as the second parameter allows any callable, it's possible to call from Twig any statically callable PHP function/method. It's not possible as customer to provide any Twig code, the attacker would require access to Administration to exploit it using Mail templates or using App Scripts. Update	https://github.com/shopware/core/commit/04183e0c02af3b404eb7d52c683734bfe0595038, https://github.com/shopware/core/commit/a784aa1cec0624e36e0ee4d41aeebaed40e0442f, https://github.com/shopware/shopware/commit/8504ba7e56e53add6a1d5b9d45015e3d899cd0ac	A-SHO-SHOP-080824/1222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to Shopware 6.6.5.1 or 6.5.8.13 to receive a patch. For older versions of 6.1, 6.2, 6.3 and 6.4 corresponding security measures are also available via a plugin. **CVE ID: CVE-2024-42356**		
N/A	08-Aug-2024	5.9	Shopware is an open commerce platform. The store-API works with regular entities and not expose all fields for the public API; fields need to be marked as ApiAware in the EntityDefinition. So only ApiAware fields of the EntityDefinition will be encoded to the final JSON. Prior to versions 6.6.5.1 and 6.5.8.13, the processing of the Criteria did not considered ManyToMany associations and so they were not considered properly and the protections didn't get used. This issue cannot be reproduced with the default entities	https://github.com/shopware/core/commit/a784aa1cec0624e36e0ee4d41aeebaed40e0442f, https://github.com/shopware/core/commit/d35ee2eda5c995faeb08b3dad127eab65c64e2a2, https://github.com/shopware/shopware/commit/8504ba7e56e53add6a1d5b9d45015e3d899cd0ac	A-SHO-SHOP-080824/1223

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by Shopware, but can be triggered with extensions. Update to Shopware 6.6.5.1 or 6.5.8.13 to receive a patch. For older versions of 6.2, 6.3, and 6.4, corresponding security measures are also available via a plugin. **CVE ID: CVE-2024-42354**		
Vendor: siamonhasan					
Product: warehouse_inventory_system					
Affected Version(s): 1.0					
Cross-Site Request Forgery (CSRF)	04-Aug-2024	8.8	A vulnerability was found in OSWAPP Warehouse Inventory System 1.0/2.0. It has been classified as problematic. Affected is an unknown function of the file /edit_account.php. The manipulation leads to cross-site request forgery. 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-273552.	N/A	A-SIA-WARE-080824/1224

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7459		
Cross-Site Request Forgery (CSRF)	04-Aug-2024	8.8	A vulnerability was found in OSWAPP Warehouse Inventory System 1.0/2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /change_password.php. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273553 was assigned to this vulnerability. **CVE ID: CVE-2024-7460**	N/A	A-SIA-WARE-080824/1225
Affected Version(s): 2.0					
Cross-Site Request Forgery (CSRF)	04-Aug-2024	8.8	A vulnerability was found in OSWAPP Warehouse Inventory System 1.0/2.0. It has been classified as problematic. Affected is an unknown function of the file /edit_account.php.	N/A	A-SIA-WARE-080824/1226

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation leads to cross-site request forgery. 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-273552. **CVE ID: CVE-2024-7459**		
Cross-Site Request Forgery (CSRF)	04-Aug-2024	8.8	A vulnerability was found in OSWAPP Warehouse Inventory System 1.0/2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /change_password.php. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273553 was assigned to this vulnerability. **CVE ID: CVE-2024-7460**	N/A	A-SIA-WARE-080824/1227

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Siemens					
Product: location_intelligence					
Affected Version(s): * Up to (excluding) 4.4					
Inadequate Encryption Strength	13-Aug-2024	7.5	A vulnerability has been identified in Location Intelligence family (All versions < V4.4). The web server of affected products is configured to support weak ciphers by default. This could allow an unauthenticated attacker in an on-path position to to read and modify any data passed over the connection between legitimate clients and the affected device. **CVE ID: CVE-2024-41681**	https://cert-portal.siemens.com/productcert/html/ssa-720392.html	A-SIE-LOCA-080824/1228
Improper Restriction of Excessive Authentication Attempts	13-Aug-2024	5.3	A vulnerability has been identified in Location Intelligence family (All versions < V4.4). Affected products do not properly enforce restriction of excessive authentication attempts. This could allow an unauthenticated remote attacker to conduct brute force	https://cert-portal.siemens.com/productcert/html/ssa-720392.html	A-SIE-LOCA-080824/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against legitimate user passwords. **CVE ID: CVE-2024-41682**		
Weak Password Requirements	13-Aug-2024	5.3	A vulnerability has been identified in Location Intelligence family (All versions < V4.4). Affected products do not properly enforce a strong user password policy. This could facilitate a brute force attack against legitimate user passwords. **CVE ID: CVE-2024-41683**	https://cert-portal.siemens.com/productcert/html/ssa-720392.html	A-SIE-LOCA-080824/1230
Product: sinec_nms					
Affected Version(s): * Up to (excluding) 3.0					
N/A	13-Aug-2024	9.1	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application does not properly validate user input to a privileged command queue. This could allow an authenticated attacker to execute OS commands with elevated privileges. **CVE ID: CVE-2024-41940**	https://cert-portal.siemens.com/productcert/html/ssa-784301.html	A-SIE-SINE-080824/1231

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	13-Aug-2024	8.8	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application does not properly enforce authorization checks. This could allow an authenticated attacker to bypass the checks and elevate their privileges on the application. **CVE ID: CVE-2024-41939**	https://cert-portal.siemens.com/productcert/html/ssa-784301.html	A-SIE-SINE-080824/1232
N/A	13-Aug-2024	7.8	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application executes a subset of its services as `NT AUTHORITY\SYSTEM`. This could allow a local attacker to execute operating system commands with elevated privileges. **CVE ID: CVE-2024-36398**	https://cert-portal.siemens.com/productcert/html/ssa-784301.html	A-SIE-SINE-080824/1233
Incorrect Authorization	13-Aug-2024	4.3	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application does not properly	https://cert-portal.siemens.com/productcert/html/ssa-784301.html	A-SIE-SINE-080824/1234

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enforce authorization checks. This could allow an authenticated attacker to bypass the checks and modify settings in the application without authorization. **CVE ID: CVE-2024-41941**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Aug-2024	3.8	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The importCertificate function of the SINEC NMS Control web application contains a path traversal vulnerability. This could allow an authenticated attacker it to delete arbitrary certificate files on the drive SINEC NMS is installed on. **CVE ID: CVE-2024-41938**	https://cert-portal.siemens.com/productcert/html/ssa-784301.html	A-SIE-SINE-080824/1235
Product: sinec_traffic_analyzer					
Affected Version(s): * Up to (excluding) 2.0					
Improper Restriction of Excessive Authentica	13-Aug-2024	7.5	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions	https://cert-portal.siemens.com/productcert/html/ssa-716317.html	A-SIE-SINE-080824/1236

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			< V2.0). The affected application do not properly enforce restriction of excessive authentication attempts. This could allow an unauthenticated attacker to conduct brute force attacks against legitimate user credentials or keys. **CVE ID: CVE-2024-41904**		
N/A	13-Aug-2024	7.2	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application mounts the container's root filesystem with read and write privileges. This could allow an attacker to alter the container's filesystem leading to unauthorized modifications and data corruption. **CVE ID: CVE-2024-41903**	https://cert-portal.siemens.com/productcert/html/ssa-716317.html	A-SIE-SINE-080824/1237
N/A	13-Aug-2024	6.5	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-	https://cert-portal.siemens.com/productcert	A-SIE-SINE-080824/1238

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0BA0) (All versions < V2.0). The affected application do not have access control for accessing the files. This could allow an authenticated attacker with low privilege's to get access to sensitive information. **CVE ID: CVE-2024-41905**	/html/ssa-716317.html	
N/A	13-Aug-2024	6.5	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application does not properly handle cacheable HTTP responses in the web service. This could allow an attacker to read and modify data stored in the local cache. **CVE ID: CVE-2024-41906**	https://cert-portal.siemens.com/productcert/html/ssa-716317.html	A-SIE-SINE-080824/1239
N/A	13-Aug-2024	5.4	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application is missing general HTTP security	https://cert-portal.siemens.com/productcert/html/ssa-716317.html	A-SIE-SINE-080824/1240

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			headers in the web server. This could allow an attacker to make the servers more prone to clickjacking attack. **CVE ID: CVE-2024-41907**		
Vendor: Solarwinds					
Product: web_help_desk					
Affected Version(s): * Up to (including) 12.8.2					
Deserialization of Untrusted Data	13-Aug-2024	9.8	SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. While it was reported as an unauthenticated vulnerability, SolarWinds has been unable to reproduce it without authentication after thorough testing. However, out of an abundance of caution, we recommend all Web Help Desk	https://support.solarwinds.com/SuccessCenter/s/article/WHD-12-8-3-Hotfix-1, https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28986	A-SOL-WEB_-080824/1241

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			customers apply the patch, which is now available. **CVE ID: CVE-2024-28986**		
Affected Version(s): 12.8.3					
Deserialization of Untrusted Data	13-Aug-2024	9.8	SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. While it was reported as an unauthenticated vulnerability, SolarWinds has been unable to reproduce it without authentication after thorough testing. However, out of an abundance of caution, we recommend all Web Help Desk customers apply the patch, which is now available. **CVE ID: CVE-2024-28986**	https://support.solarwinds.com/SuccessCenter/s/article/WHD-12-8-3-Hotfix-1, https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28986	A-SOL-WEB_-080824/1242

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: SSH					
Product: privx					
Affected Version(s): 33.0					
N/A	06-Aug-2024	9.1	PrivX before 34.0 allows data exfiltration and denial of service via the REST API. This is fixed in minor versions 33.1, 32.3, 31.3, and later, and in major version 34.0 and later, **CVE ID: CVE-2024-30170**	https://info.ssh.com/improper-input-validation-faq, https://privx.docs.ssh.com/docs/security	A-SSH-PRIV-080824/1243
Affected Version(s): From (including) 22.0 Up to (excluding) 31.3					
N/A	06-Aug-2024	9.1	PrivX before 34.0 allows data exfiltration and denial of service via the REST API. This is fixed in minor versions 33.1, 32.3, 31.3, and later, and in major version 34.0 and later, **CVE ID: CVE-2024-30170**	https://info.ssh.com/improper-input-validation-faq, https://privx.docs.ssh.com/docs/security	A-SSH-PRIV-080824/1244
Affected Version(s): From (including) 32.0 Up to (excluding) 32.3					
N/A	06-Aug-2024	9.1	PrivX before 34.0 allows data exfiltration and denial of service via the REST API. This is fixed in minor versions 33.1, 32.3, 31.3, and later, and in major version 34.0 and later,	https://info.ssh.com/improper-input-validation-faq, https://privx.docs.ssh.com/docs/security	A-SSH-PRIV-080824/1245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-30170		
Vendor: steve-community					
Product: steve					
Affected Version(s): * Up to (including) 3.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	6.1	SteVe is an open platform that implements different version of the OCPP protocol for Electric Vehicle charge points, acting as a central server for management of registered charge points. Attackers can inject arbitrary HTML and Javascript code via WebSockets leading to persistent Cross-Site Scripting in the SteVe management interface. **CVE ID: CVE-2024-21550**	https://github.com/steve-community/steve/commit/a79983f843c37705182c8f54eba060c1dce3b6d1, https://github.com/steve-community/steve/issues/1526, https://github.com/steve-community/steve/pull/1527	A-STE-STEV-080824/1246
Affected Version(s): 3.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	6.1	SteVe is an open platform that implements different version of the OCPP protocol for Electric Vehicle charge points, acting as a central server for management of registered charge points. Attackers can inject arbitrary	https://github.com/steve-community/steve/commit/a79983f843c37705182c8f54eba060c1dce3b6d1, https://github.com/steve-community/steve/issues/1526, https://github.com/steve-	A-STE-STEV-080824/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTML and Javascript code via WebSockets leading to persistent Cross-Site Scripting in the SteVe management interface. **CVE ID: CVE-2024-21550**	community/steve/pull/1527	
Affected Version(s): 3.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	6.1	SteVe is an open platform that implements different version of the OCPP protocol for Electric Vehicle charge points, acting as a central server for management of registered charge points. Attackers can inject arbitrary HTML and Javascript code via WebSockets leading to persistent Cross-Site Scripting in the SteVe management interface. **CVE ID: CVE-2024-21550**	https://github.com/steve-community/steve/commit/a79983f843c37705182c8f54eba060c1dce3b6d1, https://github.com/steve-community/steve/issues/1526, https://github.com/steve-community/steve/pull/1527	A-STE-STEV-080824/1248
Vendor: Symphony-cms					
Product: symphony_cms					
Affected Version(s): * Up to (including) 2.7.10					
Improper Neutralization of Input During	13-Aug-2024	4.8	symphonycms <=2.7.10 is vulnerable to Cross Site Scripting (XSS)	N/A	A-SYM-SYMP-080824/1249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			in the Comment component for articles. **CVE ID: CVE-2024-41614**		
Affected Version(s): 2.7.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Aug-2024	5.4	A Cross Site Scripting (XSS) vulnerability in Symphony CMS 2.7.10 allows remote attackers to inject arbitrary web script or HTML by editing note. **CVE ID: CVE-2024-41613**	N/A	A-SYM-SYMP-080824/1250
Vendor: tamparongj_03					
Product: online_graduate_tracer_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Aug-2024	8.8	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /tracking/admin/view_itprofile.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to	N/A	A-TAM-ONLI-080824/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. **CVE ID: CVE-2024-7810**		
N/A	15-Aug-2024	7.5	A vulnerability, which was classified as problematic, has been found in SourceCodester Online Graduate Tracer System 1.0. This issue affects some unknown processing of the file /tracking/admin/export_it.php. The manipulation leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7842**	N/A	A-TAM-ONLI-080824/1252
N/A	15-Aug-2024	7.5	A vulnerability, which was classified as problematic, was found in SourceCodester Online Graduate Tracer System 1.0. Affected is an unknown function of the file /tracking/admin/exportcs.php. The manipulation leads	N/A	A-TAM-ONLI-080824/1253

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to information disclosure. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7843**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Aug-2024	5.4	A vulnerability has been found in SourceCodester Online Graduate Tracer System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /tracking/admin/add_acc.php. The manipulation of the argument name/user/position leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7844**	N/A	A-TAM-ONLI-080824/1254
N/A	15-Aug-2024	5.3	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0.	N/A	A-TAM-ONLI-080824/1255

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /tracking/nbproject/. The manipulation leads to exposure of information through directory listing. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7809**		
Vendor: typora					
Product: typora					
Affected Version(s): * Up to (excluding) 1.9.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	6.1	Typora before 1.9.3 Markdown editor has a cross-site scripting (XSS) vulnerability via the Mermaid component. **CVE ID: CVE-2024-41481**	N/A	A-TYP-TYPO-080824/1256
Improper Neutralization of Input During Web Page Generation	12-Aug-2024	6.1	Typora before 1.9.3 Markdown editor has a cross-site scripting (XSS) vulnerability via	N/A	A-TYP-TYPO-080824/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			the MathJax component. **CVE ID: CVE-2024-41482**		
Vendor: veribase					
Product: order_management					
Affected Version(s): * Up to (excluding) 4.010.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	9.8	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Veribilim Software Veribase Order Management allows OS Command Injection.This issue affects Veribase Order Management: before v4.010.2. **CVE ID: CVE-2024-6917**	N/A	A-VER-ORDE-080824/1258
Vendor: VIM					
Product: vim					
Affected Version(s): * Up to (excluding) 9.1.0647					
Double Free	01-Aug-2024	5.3	Vim is an open source command line text editor. Vim < v9.1.0647 has double free in src/alloc.c:616. When closing a window, the corresponding tagstack data will	https://github.com/vim/vim/commit/8a0bbe7b8aad6f8da28dee218c01bc8a0185a, https://github.com/vim/vim/security/advisorie	A-VIM-VIM-080824/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be cleared and freed. However a bit later, the quickfix list belonging to that window will also be cleared and if that quickfix list points to the same tagstack data, Vim will try to free it again, resulting in a double-free/use-after-free access exception. Impact is low since the user must intentionally execute vim with several non-default flags, but it may cause a crash of Vim. The issue has been fixed as of Vim patch v9.1.0647 **CVE ID: CVE-2024-41957**	s/GHSA-f9cr-gv85-hcr4	
Affected Version(s): * Up to (excluding) 9.1.0648					
Double Free	01-Aug-2024	4.2	Vim is an open source command line text editor. double-free in dialog_changed() in Vim < v9.1.0648. When abandoning a buffer, Vim may ask the user what to do with the modified buffer. If the user wants the changed buffer to be saved, Vim may create a new	https://github.com/vim/vim/commit/b29f4abcd4b3382fa746edd1d0562b7b48c, https://github.com/vim/vim/security/advisories/GHSA-46pw-v7qw-xc2f	A-VIM-VIM-080824/1260

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Untitled file, if the buffer did not have a name yet. However, when setting the buffer name to Unnamed, Vim will falsely free a pointer twice, leading to a double-free and possibly later to a heap-use-after-free, which can lead to a crash. The issue has been fixed as of Vim patch v9.1.0648. **CVE ID: CVE-2024-41965**		
Vendor: wurmlab					
Product: sequenceserver					
Affected Version(s): * Up to (excluding) 3.1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Aug-2024	9.8	SequenceServer lets you rapidly set up a BLAST+ server with an intuitive user interface for personal or group use. Several HTTP endpoints did not properly sanitize user input and/or query parameters. This could be exploited to inject and run unwanted shell commands. This vulnerability has been fixed in 3.1.2. **CVE ID: CVE-2024-42360**	https://github.com/wurmlab/sequenceserver/commit/457e52709f7f9ed2fceed59b3db564cb50785dba, https://github.com/wurmlab/sequenceserver/security/advisories/GHSA-qv32-5wm2-p32h	A-WUR-SEQU-080824/1261

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: xpdfreader					
Product: xpdf					
Affected Version(s): * Up to (including) 4.05					
Uncontrolled Recursion	15-Aug-2024	5.5	In Xpdf 4.05 (and earlier), a PDF object loop in a pattern resource leads to infinite recursion and a stack overflow. **CVE ID: CVE-2024-7866**	https://www.xpdfreader.com/security-bug/object-loops.html	A-XPD-XPDF-080824/1262
Vendor: xuxueli					
Product: xxl-job					
Affected Version(s): 2.4.1					
Incorrect Default Permissions	15-Aug-2024	8.8	Insecure Permissions vulnerability in xxl-job v.2.4.1 allows a remote attacker to execute arbitrary code via the Sub-Task ID component. **CVE ID: CVE-2024-42681**	N/A	A-XUX-XXL--080824/1263
Vendor: yonle					
Product: bostr					
Affected Version(s): * Up to (excluding) 3.0.10					
N/A	01-Aug-2024	6.3	Bostr is an nostr relay aggregator proxy that acts like a regular nostr relay. bostr let everyone in even having authorized_keys being set when noscraper is set to true. This	https://github.com/Yonle/bostr/commit/49181f4ec9ae1472c6675cab56bbc01e723855af, https://github.com/Yonle/bostr/security/advisories/GHSA-5cf7-cxrf-mq73	A-YON-BOST-080824/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is fixed in 3.0.10. **CVE ID: CVE-2024-41962**		
Vendor: Zimbra					
Product: collaboration					
Affected Version(s): 9.0.0					
Improper Handling of Exceptional Conditions	12-Aug-2024	7.8	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. The zmmailboxdmgr binary, a component of ZCS, is intended to be executed by the zimbra user with root privileges for specific mailbox operations. However, an attacker can escalate privileges from the zimbra user to root, because of improper handling of input arguments. An attacker can execute arbitrary commands with elevated privileges, leading to local privilege escalation. **CVE ID: CVE-2024-27442**	N/A	A-ZIM-COLL-080824/1265
Improper Limitation of a Pathname	12-Aug-2024	7.5	An issue was discovered in Zimbra Collaboration (ZCS)	N/A	A-ZIM-COLL-080824/1266

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			9.0 and 10.0. The vulnerability involves unauthenticated local file inclusion (LFI) in a web application, specifically impacting the handling of the packages parameter. Attackers can exploit this flaw to include arbitrary local files without authentication, potentially leading to unauthorized access to sensitive information. The vulnerability is limited to files within a specific directory. **CVE ID: CVE-2024-33535**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	6.1	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. A Cross-Site Scripting (XSS) vulnerability exists in the CalendarInvite feature of the Zimbra webmail classic user interface, because of improper input validation in the handling of the	N/A	A-ZIM-COLL-080824/1267

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calendar header. An attacker can exploit this via an email message containing a crafted calendar header with an embedded XSS payload. When a victim views this message in the Zimbra webmail classic interface, the payload is executed in the context of the victim's session, potentially leading to execution of arbitrary JavaScript code. **CVE ID: CVE-2024-27443**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	5.4	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0, issue 1 of 2. A reflected cross-site scripting (XSS) vulnerability has been identified in the Zimbra webmail admin interface. This vulnerability occurs due to inadequate input validation of the packages parameter, allowing an authenticated attacker to inject	N/A	A-ZIM-COLL-080824/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and execute arbitrary JavaScript code within the context of another user's browser session. By uploading a malicious JavaScript file and crafting a URL containing its location in the packages parameter, the attacker can exploit this vulnerability. Subsequently, when another user visits the crafted URL, the malicious JavaScript code is executed. **CVE ID: CVE-2024-33533**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	5.4	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. The vulnerability occurs due to inadequate input validation of the res parameter, allowing an authenticated attacker to inject and execute arbitrary JavaScript code within the context of another user's browser session. By	N/A	A-ZIM-COLL-080824/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uploading a malicious JavaScript file, accessible externally, and crafting a URL containing its location in the res parameter, the attacker can exploit this vulnerability. Subsequently, when another user visits the crafted URL, the malicious JavaScript code is executed. **CVE ID: CVE-2024-33536**		
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.7					
Improper Handling of Exceptional Conditions	12-Aug-2024	7.8	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. The zmmailboxdmgr binary, a component of ZCS, is intended to be executed by the zimbra user with root privileges for specific mailbox operations. However, an attacker can escalate privileges from the zimbra user to root, because of improper handling of input arguments. An attacker can	N/A	A-ZIM-COLL-080824/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands with elevated privileges, leading to local privilege escalation. **CVE ID: CVE-2024-27442**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2024	6.1	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. A Cross-Site Scripting (XSS) vulnerability exists in the CalendarInvite feature of the Zimbra webmail classic user interface, because of improper input validation in the handling of the calendar header. An attacker can exploit this via an email message containing a crafted calendar header with an embedded XSS payload. When a victim views this message in the Zimbra webmail classic interface, the payload is executed in the context of the victim's session, potentially leading to execution of	N/A	A-ZIM-COLL-080824/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary JavaScript code. **CVE ID: CVE-2024-27443**		
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. The vulnerability involves unauthenticated local file inclusion (LFI) in a web application, specifically impacting the handling of the packages parameter. Attackers can exploit this flaw to include arbitrary local files without authentication, potentially leading to unauthorized access to sensitive information. The vulnerability is limited to files within a specific directory. **CVE ID: CVE-2024-33535**	N/A	A-ZIM-COLL-080824/1272
Improper Neutralization of Input During Web Page Generation	12-Aug-2024	5.4	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0, issue 1 of 2. A reflected	N/A	A-ZIM-COLL-080824/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			cross-site scripting (XSS) vulnerability has been identified in the Zimbra webmail admin interface. This vulnerability occurs due to inadequate input validation of the packages parameter, allowing an authenticated attacker to inject and execute arbitrary JavaScript code within the context of another user's browser session. By uploading a malicious JavaScript file and crafting a URL containing its location in the packages parameter, the attacker can exploit this vulnerability. Subsequently, when another user visits the crafted URL, the malicious JavaScript code is executed. **CVE ID: CVE-2024-33533**		
Improper Neutralization of Input During	12-Aug-2024	5.4	An issue was discovered in Zimbra Collaboration (ZCS)	N/A	A-ZIM-COLL-080824/1274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			9.0 and 10.0. The vulnerability occurs due to inadequate input validation of the res parameter, allowing an authenticated attacker to inject and execute arbitrary JavaScript code within the context of another user's browser session. By uploading a malicious JavaScript file, accessible externally, and crafting a URL containing its location in the res parameter, the attacker can exploit this vulnerability. Subsequently, when another user visits the crafted URL, the malicious JavaScript code is executed. **CVE ID: CVE-2024-33536**		
Vendor: Zohocorp					
Product: manageengine_adaudit_plus					
Affected Version(s): * Up to (excluding) 8.0					
Improper Neutralization of Special Elements	12-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8003 are	https://www.manageengine.com/products/active-directory-	A-ZOH-MANA-080824/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			vulnerable to authenticated SQL Injection in aggregate reports' search option. **CVE ID: CVE-2024-36034**	audit/sqlfix-8003.html	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8003 are vulnerable to authenticated SQL Injection in user session recording. **CVE ID: CVE-2024-36035**	https://www.manageengine.com/products/active-directory-audit/sqlfix-8003.html	A-ZOH-MANA-080824/1276
Affected Version(s): * Up to (excluding) 8.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8110 are vulnerable to authenticated SQL Injection in attack surface analyzer's export option. **CVE ID: CVE-2024-5487**	https://www.manageengine.com/products/active-directory-audit/cve-2024-5487.html	A-ZOH-MANA-080824/1277
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8110 are vulnerable to authenticated SQL Injection in file auditing configuration.	https://www.manageengine.com/products/active-directory-audit/cve-2024-5527.html	A-ZOH-MANA-080824/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-5527		
Affected Version(s): 8.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8003 are vulnerable to authenticated SQL Injection in aggregate reports' search option. **CVE ID: CVE-2024-36034**	https://www.manageengine.com/products/active-directory-audit/sqlfix-8003.html	A-ZOH-MANA-080824/1279
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8003 are vulnerable to authenticated SQL Injection in user session recording. **CVE ID: CVE-2024-36035**	https://www.manageengine.com/products/active-directory-audit/sqlfix-8003.html	A-ZOH-MANA-080824/1280
Affected Version(s): 8.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8110 are vulnerable to authenticated SQL Injection in attack surface analyzer's export option. **CVE ID: CVE-2024-5487**	https://www.manageengine.com/products/active-directory-audit/cve-2024-5487.html	A-ZOH-MANA-080824/1281
Improper Neutralizat	12-Aug-2024	8.8	Zohocorp ManageEngine	https://www.manageengine.co	A-ZOH-MANA-080824/1282

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			ADAudit Plus versions below 8110 are vulnerable to authenticated SQL Injection in file auditing configuration. **CVE ID: CVE-2024-5527**	m/products/active-directory-audit/cve-2024-5527.html	
Product: manageengine_applications_manager					
Affected Version(s): * Up to (excluding) 16.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Aug-2024	4.7	Zohocorp ManageEngine Applications Manager versions 170900 and below are vulnerable to the authenticated admin-only SQL Injection in the Create Monitor feature. **CVE ID: CVE-2024-5678**	https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2024-5678.html	A-ZOH-MANA-080824/1283
Affected Version(s): 16.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Aug-2024	4.7	Zohocorp ManageEngine Applications Manager versions 170900 and below are vulnerable to the authenticated admin-only SQL Injection in the Create Monitor feature. **CVE ID: CVE-2024-5678**	https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2024-5678.html	A-ZOH-MANA-080824/1284

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 17.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Aug-2024	4.7	Zohocorp ManageEngine Applications Manager versions 170900 and below are vulnerable to the authenticated admin-only SQL Injection in the Create Monitor feature. **CVE ID: CVE-2024-5678**	https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2024-5678.html	A-ZOH-MANA-080824/1285
Vendor: zscaler					
Product: client_connector					
Affected Version(s): * Up to (excluding) 4.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	An Improper Input Validation vulnerability in Zscaler Client Connector on MacOS allows OS Command Injection. This issue affects Zscaler Client Connector on MacOS <4.2. **CVE ID: CVE-2024-23483**	https://help.zscaler.com/client-connector/client-connector-app-release-summary-2023?applicable_category=macos&applicable_version=4.2	A-ZSC-CLIE-080824/1286
Improper Verification of Cryptographic Signature	06-Aug-2024	7.8	The Zscaler Updater process does not validate the digital signature of the installer before execution, allowing arbitrary code to be locally executed. This affects Zscaler	https://help.zscaler.com/client-connector/client-connector-app-release-summary-2023?applicable_category=macos&applicable_version=4.2	A-ZSC-CLIE-080824/1287

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Client Connector on MacOS <4.2. **CVE ID: CVE-2024-23460**		
Affected Version(s): * Up to (excluding) 4.2.0.190					
Origin Validation Error	06-Aug-2024	7.8	While copying individual autoupdater log files, reparse point check was missing which could result into crafted attacks, potentially leading to a local privilege escalation. This issue affects Zscaler Client Connector on Windows <4.2.0.190. **CVE ID: CVE-2024-23458**	https://help.zscaler.com/client-connector/client-connector-app-release-summary-2023?applicable_category=windows&applicable_version=4.2.0.190	A-ZSC-CLIE-080824/1288
Improper Verification of Cryptographic Signature	06-Aug-2024	7.5	Anti-tampering can be disabled under certain conditions without signature validation. This affects Zscaler Client Connector <4.2.0.190 with anti-tampering enabled. **CVE ID: CVE-2024-23456**	https://help.zscaler.com/client-connector/client-connector-app-release-summary-2023?applicable_category=windows&applicable_version=4.2.0.190	A-ZSC-CLIE-080824/1289
Improper Verification of Cryptographic Signature	06-Aug-2024	6.5	An Improper Validation of signature in Zscaler Client Connector on Windows allows an authenticated user to disable anti-tampering. This issue affects Client	https://help.zscaler.com/client-connector/client-connector-app-release-summary-2023?applicable_category=windows&applicabl	A-ZSC-CLIE-080824/1290

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connector on Windows <4.2.0.190. **CVE ID: CVE-2023-28806**	e_version=4.2.0.190	
Affected Version(s): * Up to (excluding) 4.2.1					
N/A	06-Aug-2024	4.9	In certain cases, Zscaler Internet Access (ZIA) can be disabled by PowerShell commands with admin rights. This affects Zscaler Client Connector on Windows <4.2.1 **CVE ID: CVE-2024-23464**	https://help.zscaler.com/client-connector/client-connector-app-release-summary-2023?applicable_category=Windows&applicable_version=4.2.1	A-ZSC-CLIE-080824/1291
Hardware					
Vendor: airveda					
Product: pm2.5_pm10_monitor					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	12-Aug-2024	6.5	This vulnerability exists in Airveda Air Quality Monitor PM2.5 PM10 due to transmission of sensitive information in plain text during AP pairing mode. An attacker in close proximity could exploit this vulnerability by capturing Wi-Fi traffic of Airveda-AP.	N/A	H-AIR-PM2.-080824/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability could allow the attacker to cause Evil Twin attack on the targeted system. **CVE ID: CVE-2024-7408**		
Vendor: alientechnology					
Product: alr-f800					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Aug-2024	9.8	A vulnerability was found in Alien Technology ALR-F800 up to 19.10.24.00. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/system.html. The manipulation of the argument uploadedFile with the input ;whoami leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did	N/A	H-ALI-ALR--080824/1293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID: CVE-2024-7580**		
Vendor: annke					
Product: crater_2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	8.8	An OS command injection vulnerability in the ccm_debug component of MIPC Camera firmware prior to v5.4.1.240424171021 allows attackers within the same network to execute arbitrary code via a crafted HTML request. **CVE ID: CVE-2024-39091**	N/A	H-ANN-CRAT-080824/1294
Vendor: Dlink					
Product: di-8100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	15-Aug-2024	9.8	A vulnerability was found in D-Link DI-8100 16.07. It has been classified as critical. This affects the function upgrade_filter_asp of the file upgrade_filter.asp. The manipulation of the argument path leads to command injection. It is possible to	N/A	H-DLI-DI-8-080824/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7833**		
Product: dir-300					
Affected Version(s): a					
Use of Hard-coded Credentials	06-Aug-2024	9.8	D-Link DIR-300 REVA FIRMWARE v1.06B05_WW contains hardcoded credentials in the Telnet service. **CVE ID: CVE-2024-41616**	N/A	H-DLI-DIR--080824/1296
Product: dnr-202l					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1297

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1298

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1300

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dnr-322l					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1303

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1305

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dnr-326					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1308

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1310

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--080824/1311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-1100-4					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1312

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1313

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1315

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-120					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1317

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1318

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1320

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1321

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-1200-05					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1322

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1323

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1325

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1326

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-1550-04					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1327

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1328

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1330

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1331

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-315l					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1333

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1335

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-320					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1337

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1338

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1340

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1341

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-320l					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1342

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1343

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1345

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1346

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-320lw					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1348

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1350

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-321					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1353

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1355

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1356

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-323					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1357

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1358

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1360

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1361

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-325					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1363

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1365

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1366

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-326					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1367

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1368

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1370

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-327l					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1373

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1375

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1376

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-340l					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1377

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1378

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1380

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-343					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1382

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1383

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1385

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1386

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-345					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1387

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1388

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1390

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1391

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-726-4					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1392

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1393

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7830		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1395

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7831**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--080824/1396

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Vendor: Edimax					
Product: ic-5150w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.8	A vulnerability was found in Edimax IC-6220DC and IC-5150W up to 3.06. It has been rated as critical. Affected by this issue is the function cgiFormString of the file ipcam_cgi. The manipulation of the argument host leads to command injection. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	H-EDI-IC-5-080824/1397

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7616		
Product: ic-6220dc					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.8	A vulnerability was found in Edimax IC-6220DC and IC-5150W up to 3.06. It has been rated as critical. Affected by this issue is the function cgiFormString of the file ipcam_cgi. The manipulation of the argument host leads to command injection. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7616**	N/A	H-EDI-IC-6-080824/1398
Vendor: F5					
Product: r2000					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization.	https://my.f5.com/manage/s/article/K000138833	H-F5-R200-080824/1399

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**		
Product: r4000					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	14-Aug-2024	7.5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2024-41727**	https://my.f5.com/manage/s/article/K000138833	H-F5-R400-080824/1400
Vendor: gl-inet					
Product: a1300					
Affected Version(s): -					
Improper Restriction of Excessive Authentica	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT130	N/A	H-GL--A130-080824/1401

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell	N/A	H-GL--A130-080824/1402

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	H-GL--A130-080824/1403
Improper Neutralization of Special Elements in Output Used by a Downstream Component	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750	N/A	H-GL--A130-080824/1404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows	N/A	H-GL--A130-080824/1405

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: ap1300					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--AP13-080824/1406
Improper Limitation of a Pathname to a Restricted Directory	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11,	N/A	H-GL--AP13-080824/1407

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface	N/A	H-GL--AP13-080824/1408

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	H-GL--AP13-080824/1409
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-	N/A	H-GL--AP13-080824/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: ar300m					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300	N/A	H-GL--AR30-080824/1411

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	H-GL--AR30-080824/1412
Improper Neutralization of Special Elements used in an	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750	N/A	H-GL--AR30-080824/1413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_ config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This	N/A	H-GL--AR30-080824/1414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	H-GL--AR30-080824/1415

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ar300m16					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--AR30-080824/1416
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to	N/A	H-GL--AR30-080824/1417

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	H-GL--AR30-080824/1418
Improper Neutralization of Special Elements in Output	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750	N/A	H-GL--AR30-080824/1419

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Used by a Downstream Component ('Injection')			v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13,	N/A	H-GL--AR30-080824/1420

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: ar750					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--AR75-080824/1421

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	H-GL--AR75-080824/1422
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and	N/A	H-GL--AR75-080824/1423

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data.	N/A	H-GL--AR75-080824/1424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39227		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	H-GL--AR75-080824/1425
Product: ar750s					
Affected Version(s): -					
Improper Restriction of Excessive Authentica	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750	N/A	H-GL--AR75-080824/1426

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API.	N/A	H-GL--AR75-080824/1427

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39226		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	H-GL--AR75-080824/1428
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300	N/A	H-GL--AR75-080824/1429

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept	N/A	H-GL--AR75-080824/1430

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: ax1800					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--AX18-080824/1431
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	H-GL--AX18-080824/1432

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_	N/A	H-GL--AX18-080824/1433

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	H-GL--AX18-080824/1434
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT130	N/A	H-GL--AX18-080824/1435

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/M V1000W/USB150/ N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: axt1800					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and	N/A	H-GL--AXT1-080824/1436

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	H-GL--AXT1-080824/1437
Improper Neutralization of Special Elements used in an OS	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11,	N/A	H-GL--AXT1-080824/1438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_ config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability	N/A	H-GL--AXT1-080824/1439

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	H-GL--AXT1-080824/1440

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: b1300					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--B130-080824/1441
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to	N/A	H-GL--B130-080824/1442

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	H-GL--B130-080824/1443
Improper Neutralization of Special Elements in Output	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750	N/A	H-GL--B130-080824/1444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Used by a Downstream Component ('Injection')			v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13,	N/A	H-GL--B130-080824/1445

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: b2200					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--B220-080824/1446

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	H-GL--B220-080824/1447
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and	N/A	H-GL--B220-080824/1448

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data.	N/A	H-GL--B220-080824/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39227		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	H-GL--B220-080824/1450
Product: e750					
Affected Version(s): -					
Improper Restriction of Excessive Authentica	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750	N/A	H-GL--E750-080824/1451

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API.	N/A	H-GL--E750-080824/1452

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39226		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	H-GL--E750-080824/1453
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300	N/A	H-GL--E750-080824/1454

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept	N/A	H-GL--E750-080824/1455

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: mt1300					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--MT13-080824/1456
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	H-GL--MT13-080824/1457

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_	N/A	H-GL--MT13-080824/1458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	H-GL--MT13-080824/1459
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT130	N/A	H-GL--MT13-080824/1460

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/M V1000W/USB150/ N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: mt2500					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and	N/A	H-GL--MT25-080824/1461

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	H-GL--MT25-080824/1462
Improper Neutralization of Special Elements used in an OS	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11,	N/A	H-GL--MT25-080824/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_ config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability	N/A	H-GL--MT25-080824/1464

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	H-GL--MT25-080824/1465

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt3000					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--MT30-080824/1466
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to	N/A	H-GL--MT30-080824/1467

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	H-GL--MT30-080824/1468
Improper Neutralization of Special Elements in Output	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750	N/A	H-GL--MT30-080824/1469

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Used by a Downstream Component ('Injection')			v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13,	N/A	H-GL--MT30-080824/1470

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: mt300n-v2					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--MT30-080824/1471

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	H-GL--MT30-080824/1472
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and	N/A	H-GL--MT30-080824/1473

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data.	N/A	H-GL--MT30-080824/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39227		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	H-GL--MT30-080824/1475
Product: mt6000					
Affected Version(s): -					
Improper Restriction of Excessive Authentica	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750	N/A	H-GL--MT60-080824/1476

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API.	N/A	H-GL--MT60-080824/1477

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39226		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	H-GL--MT60-080824/1478
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300	N/A	H-GL--MT60-080824/1479

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept	N/A	H-GL--MT60-080824/1480

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: mv1000					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--MV10-080824/1481
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	H-GL--MV10-080824/1482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_	N/A	H-GL--MV10-080824/1483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	H-GL--MV10-080824/1484
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT130	N/A	H-GL--MV10-080824/1485

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/M V1000W/USB150/ N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: mv1000w					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and	N/A	H-GL--MV10-080824/1486

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	H-GL--MV10-080824/1487
Improper Neutralization of Special Elements used in an OS	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11,	N/A	H-GL--MV10-080824/1488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_ config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability	N/A	H-GL--MV10-080824/1489

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	H-GL--MV10-080824/1490

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: n300					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--N300-080824/1491
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to	N/A	H-GL--N300-080824/1492

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	H-GL--N300-080824/1493
Improper Neutralization of Special Elements in Output	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750	N/A	H-GL--N300-080824/1494

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Used by a Downstream Component ('Injection')			v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13,	N/A	H-GL--N300-080824/1495

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: s1300					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--S130-080824/1496

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	H-GL--S130-080824/1497
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and	N/A	H-GL--S130-080824/1498

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data.	N/A	H-GL--S130-080824/1499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39227		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	H-GL--S130-080824/1500
Product: sf1200					
Affected Version(s): -					
Improper Restriction of Excessive Authentica	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750	N/A	H-GL--SF12-080824/1501

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API.	N/A	H-GL--SF12-080824/1502

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39226		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	H-GL--SF12-080824/1503
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300	N/A	H-GL--SF12-080824/1504

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept	N/A	H-GL--SF12-080824/1505

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: sft1200					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--SFT1-080824/1506
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	H-GL--SFT1-080824/1507

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_	N/A	H-GL--SFT1-080824/1508

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	H-GL--SFT1-080824/1509
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT130	N/A	H-GL--SFT1-080824/1510

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/M V1000W/USB150/ N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: usb150					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and	N/A	H-GL--USB1-080824/1511

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	H-GL--USB1-080824/1512
Improper Neutralization of Special Elements used in an OS	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11,	N/A	H-GL--USB1-080824/1513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_ config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability	N/A	H-GL--USB1-080824/1514

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	H-GL--USB1-080824/1515

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: x3000					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--X300-080824/1516
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to	N/A	H-GL--X300-080824/1517

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	H-GL--X300-080824/1518
Improper Neutralization of Special Elements in Output	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750	N/A	H-GL--X300-080824/1519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Used by a Downstream Component ('Injection')			v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13,	N/A	H-GL--X300-080824/1520

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: x300b					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--X300-080824/1521

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	H-GL--X300-080824/1522
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and	N/A	H-GL--X300-080824/1523

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data.	N/A	H-GL--X300-080824/1524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39227		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	H-GL--X300-080824/1525
Product: x750					
Affected Version(s): -					
Improper Restriction of Excessive Authentica	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750	N/A	H-GL--X750-080824/1526

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API.	N/A	H-GL--X750-080824/1527

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39226		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	H-GL--X750-080824/1528
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300	N/A	H-GL--X750-080824/1529

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept	N/A	H-GL--X750-080824/1530

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: xe300					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	H-GL--XE30-080824/1531
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	H-GL--XE30-080824/1532

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_	N/A	H-GL--XE30-080824/1533

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	H-GL--XE30-080824/1534
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT130	N/A	H-GL--XE30-080824/1535

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/M V1000W/USB150/ N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: xe3000					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and	N/A	H-GL--XE30-080824/1536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	H-GL--XE30-080824/1537
Improper Neutralization of Special Elements used in an OS	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11,	N/A	H-GL--XE30-080824/1538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_ config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability	N/A	H-GL--XE30-080824/1539

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	H-GL--XE30-080824/1540

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: gncchome					
Product: _gncc_c2					
Affected Version(s): -					
Use of Hard-coded Credentials	15-Aug-2024	6.8	Identical Hardcoded Root Password for All Devices in GNCC's GC2 Indoor Security Camera 1080P allows an attacker with physical access to retrieve the root password for all similar devices **CVE ID: CVE-2024-31798**	N/A	H-GNC-_GNC-080824/1541
Improper Authentication	15-Aug-2024	6.8	Authentication Bypass in GNCC's GC2 Indoor Security Camera 1080P allows an attacker with physical access to gain a privileged command shell via the UART Debugging Port. **CVE ID: CVE-2024-31800**	N/A	H-GNC-_GNC-080824/1542
Cleartext Transmission of Sensitive Information	15-Aug-2024	4.6	Information Disclosure in GNCC's GC2 Indoor Security Camera 1080P allows an attacker with physical access to read the WiFi passphrase via the UART Debugging Port.	N/A	H-GNC-_GNC-080824/1543

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-31799		
Vendor: hms-networks					
Product: ewon_cosy\+					
Affected Version(s): -					
Direct Request ('Forced Browsing')	06-Aug-2024	9.1	A compromised HMS Networks Cosy+ device could be used to request a Certificate Signing Request from Talk2m for another device, resulting in an availability issue. The issue was patched on the Talk2m production server on April 18, 2024. **CVE ID: CVE-2024-33897**	https://hmsnetworks.blob.core.windows.net/nlw/docs/default-source/products/cybersecurity/security-advisory/hms-security-advisory-2024-07-29-001--ewon-several-cosy--vulnerabilities.pdf, https://www.hms-networks.com/cyber-security	H-HMS-EWON-080824/1544
Vendor: HP					
Product: poly_clariti_manager					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	06-Aug-2024	8.8	A vulnerability was discovered in the firmware builds up to 10.10.2.2 in Poly Clariti Manager devices. The firmware flaw does not properly sanitize User input. **CVE ID: CVE-2024-41913**	https://support.hp.com/us-en/document/ish_11006488-11006512-16/hpsbpy03957	H-HP-POLY-080824/1545

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	6.1	A vulnerability was discovered in the firmware builds up to 10.10.2.2 in Poly Clariti Manager devices. The firmware contained multiple XSS vulnerabilities in the version of JavaScript used. **CVE ID: CVE-2024-41910**	https://support.hp.com/us-en/document/ish_11006981-11007005-16/hpsbpy03960	H-HP-POLY-080824/1546
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	5.4	A vulnerability was discovered in the firmware builds up to 10.10.2.2 in Poly Clariti Manager devices. The flaw does not properly neutralize input during a web page generation. **CVE ID: CVE-2024-41911**	https://support.hp.com/us-en/document/ish_11006770-11006795-16/hpsbpy03959	H-HP-POLY-080824/1547
Vendor: kaongroup					
Product: ar2140					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Aug-2024	7.2	Firmware in KAON AR2140 routers prior to version 4.2.16 is vulnerable to a shell command injection via sending a crafted request to one of the endpoints. In order to exploit this vulnerability, one has to have	N/A	H-KAO-AR21-080824/1548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to the administrative portal of the router. **CVE ID: CVE-2024-3659**		
Vendor: nissan-global					
Product: altima					
Affected Version(s): 2022					
N/A	15-Aug-2024	6.5	* Unprotected privileged mode access through UDS session in the Blind Spot Detection Sensor ECU firmware in Nissan Altima (2022) allows attackers to trigger denial-of-service (DoS) by unauthorized access to the ECU's programming session. * No preconditions implemented for ECU management functionality through UDS session in the Blind Spot Detection Sensor ECU in Nissan Altima (2022) allows attackers to disrupt normal ECU operations by triggering a control command without authentication.	N/A	H-NIS-ALTI-080824/1549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-6347		
Vendor: raisecom					
Product: msg1200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90 and classified as critical. Affected by this issue is the function sslvpn_config_mod of the file /vpn/list_ip_network.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273560. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7467**	N/A	H-RAI-MSG1-080824/1550

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been classified as critical. This affects the function sslvpn_config_mod of the file /vpn/list_service_manage.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273561 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7468**	N/A	H-RAI-MSG1-080824/1551
Improper Neutralization of Special Elements	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and	N/A	H-RAI-MSG1-080824/1552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			MSG2300 3.90. It has been declared as critical. This vulnerability affects the function sslvpn_config_mod of the file /vpn/list_vpn_web_custom.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273562 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7469**		
Improper Neutralization of Special Elements used in an OS Command ('OS	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been rated as critical. This issue affects the function	N/A	H-RAI-MSG1-080824/1553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			sslvpn_config_mod of the file /vpn/vpn_template_style.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273563. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7470**		
Product: msg2100e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90 and classified as critical. Affected by this issue is the function sslvpn_config_mod of the file /vpn/list_ip_netwo	N/A	H-RAI-MSG2-080824/1554

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rk.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273560. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7467**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been classified as critical. This affects the function sslvpn_config_mod of the file /vpn/list_service_manage.php of the component Web Interface. The manipulation of the argument template/stylenum	N/A	H-RAI-MSG2-080824/1555

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273561 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7468**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been declared as critical. This vulnerability affects the function sslvpn_config_mod of the file /vpn/list_vpn_web_custom.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack can be initiated remotely.	N/A	H-RAI-MSG2-080824/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. VDB-273562 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7469**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been rated as critical. This issue affects the function sslvpn_config_mod of the file /vpn/vpn_template_style.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated	N/A	H-RAI-MSG2-080824/1557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier of this vulnerability is VDB-273563. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7470**		
Product: msg2200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90 and classified as critical. Affected by this issue is the function sslvpn_config_mod of the file /vpn/list_ip_network.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273560. NOTE: The vendor	N/A	H-RAI-MSG2-080824/1558

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7467**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been classified as critical. This affects the function sslvpn_config_mod of the file /vpn/list_service_manage.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273561 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	H-RAI-MSG2-080824/1559

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7468		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been declared as critical. This vulnerability affects the function sslvpn_config_mod of the file /vpn/list_vpn_web_custom.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273562 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7469**	N/A	H-RAI-MSG2-080824/1560
Improper Neutralizat	05-Aug-2024	9.8	A vulnerability was found in Raisecom	N/A	H-RAI-MSG2-080824/1561

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been rated as critical. This issue affects the function sslvpn_config_mod of the file /vpn/vpn_template_style.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273563. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7470**		
Product: msg2300					
Affected Version(s): -					
Improper Neutralization of Special Elements	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and	N/A	H-RAI-MSG2-080824/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			MSG2300 3.90 and classified as critical. Affected by this issue is the function sslvpn_config_mod of the file /vpn/list_ip_network.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273560. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7467**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been classified as critical. This affects the function sslvpn_config_mod of the file	N/A	H-RAI-MSG2-080824/1563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/vpn/list_service_manage.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273561 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7468**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been declared as critical. This vulnerability affects the function sslvpn_config_mod of the file /vpn/list_vpn_web_custom.php of the component Web Interface. The	N/A	H-RAI-MSG2-080824/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument template/stylenum leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273562 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7469**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been rated as critical. This issue affects the function sslvpn_config_mod of the file /vpn/vpn_template_style.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection.	N/A	H-RAI-MSG2-080824/1565

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273563. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7470**		
Vendor: Sprecher-automation					
Product: sprecon-e-c					
Affected Version(s): -					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	H-SPR-SPRE-080824/1566
Product: sprecon-e-p_dd6-2					
Affected Version(s): -					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR	H-SPR-SPRE-080824/1567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	-2407171_de.pdf	
Product: sprecon-e-p_dl6-1					
Affected Version(s): -					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	H-SPR-SPRE-080824/1568
Product: sprecon-e-p_dq6-1					
Affected Version(s): -					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	H-SPR-SPRE-080824/1569
Product: sprecon-e-p_ds6-0					
Affected Version(s): -					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	H-SPR-SPRE-080824/1570
Product: sprecon-e-t3					
Affected Version(s): -					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	H-SPR-SPRE-080824/1571
Product: sprecon-e-t3_ax-3110					
Affected Version(s): -					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments.	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	H-SPR-SPRE-080824/1572

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-6758		
Product: sprecon-edir					
Affected Version(s): -					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	H-SPR-SPRE-080824/1573
Product: sprecon-e_ap-2200					
Affected Version(s): -					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	H-SPR-SPRE-080824/1574
Product: sprecon-e_cp-2131					
Affected Version(s): -					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR	H-SPR-SPRE-080824/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	-2407171_de.pdf	
Product: sprecon-e_cp-2330					
Affected Version(s): -					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	H-SPR-SPRE-080824/1576
Product: sprecon-e_cp-2500					
Affected Version(s): -					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	H-SPR-SPRE-080824/1577
Vendor: Tenda					
Product: fh1201					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	15-Aug-2024	9.8	An issue in the handler function in /goform/telnet of Tenda FH1201 v1.2.0.14 (408) allows attackers to execute arbitrary commands via a crafted HTTP request. **CVE ID: CVE-2024-42947**	N/A	H-TEN-FH12-080824/1578
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromP2pListFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42940**	N/A	H-TEN-FH12-080824/1579
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the wanmode parameter in the fromAdvSetWan function. This vulnerability allows attackers to cause a Denial of	N/A	H-TEN-FH12-080824/1580

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42941**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the PPPOEPassword parameter in the fromAdvSetWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42943**	N/A	H-TEN-FH12-080824/1581
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromNatlimit function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42944**	N/A	H-TEN-FH12-080824/1582
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack	N/A	H-TEN-FH12-080824/1583

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the page parameter in the fromVirtualSer function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42946**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the delno parameter in the fromPptpUserSetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42948**	N/A	H-TEN-FH12-080824/1584
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the Go parameter in the fromSafeClientFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a	N/A	H-TEN-FH12-080824/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted POST request. **CVE ID: CVE-2024-42950**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the mit_pptpusrpw parameter in the fromWizardHandle function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42951**	N/A	H-TEN-FH12-080824/1586
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromqossetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42952**	N/A	H-TEN-FH12-080824/1587
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the	N/A	H-TEN-FH12-080824/1588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page parameter in the fromSafeClientFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42955**		
Product: fh1206					
Affected Version(s): -					
Out-of-bounds Write	12-Aug-2024	9.8	A vulnerability was found in Tenda FH1206 1.2.0.8(8155) and classified as critical. This issue affects the function fromGstDhcpSetSer of the file /goform/GstDhcpSetSer. The manipulation of the argument dips leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	H-TEN-FH12-080824/1589

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7613		
Out-of-bounds Write	12-Aug-2024	9.8	A vulnerability was found in Tenda FH1206 1.2.0.8(8155). It has been classified as critical. Affected is the function fromqossetting of the file /goform/qossetting. The manipulation of the argument page leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7614**	N/A	H-TEN-FH12-080824/1590
Out-of-bounds Write	12-Aug-2024	9.8	A vulnerability was found in Tenda FH1206 1.2.0.8. It has been declared as critical. Affected by this vulnerability is the function fromSafeClientFilter/fromSafeMacFilter/fromSafeUrlFilt	N/A	H-TEN-FH12-080824/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			er. The manipulation leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7615**		
N/A	15-Aug-2024	9.8	An issue in the handler function in /goform/telnet of Tenda FH1206 v02.03.01.35 allows attackers to execute arbitrary commands via a crafted HTTP request. **CVE ID: CVE-2024-42978**	N/A	H-TEN-FH12-080824/1592
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the Go parameter in the fromSafeUrlFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a	N/A	H-TEN-FH12-080824/1593

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted POST request. **CVE ID: CVE-2024-42968**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromSafeUrlFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42969**	N/A	H-TEN-FH12-080824/1594
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromSetlpBind function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42973**	N/A	H-TEN-FH12-080824/1595
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the	N/A	H-TEN-FH12-080824/1596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page parameter in the fromwebExcptype manFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42974**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromSafeClientFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42976**	N/A	H-TEN-FH12-080824/1597
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the qos parameter in the fromqossetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a	N/A	H-TEN-FH12-080824/1598

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted POST request. **CVE ID: CVE-2024-42977**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the frmL7ProtForm function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42979**	N/A	H-TEN-FH12-080824/1599
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the frmL7ImForm function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42980**	N/A	H-TEN-FH12-080824/1600
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the delno parameter in	N/A	H-TEN-FH12-080824/1601

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the fromPptpUserSetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42981**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromVirtualSer function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42982**	N/A	H-TEN-FH12-080824/1602
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the pptpPPW parameter in the fromAdvSetWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	N/A	H-TEN-FH12-080824/1603

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42983		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromP2pListFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42984**	N/A	H-TEN-FH12-080824/1604
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromNatlimit function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42985**	N/A	H-TEN-FH12-080824/1605
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the PPPOEPassword parameter in the	N/A	H-TEN-FH12-080824/1606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fromAdvSetWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42986**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the modino parameter in the fromPptpUserAdd function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42987**	N/A	H-TEN-FH12-080824/1607
Product: i22					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2024	9.8	A vulnerability classified as critical was found in Tenda i22 1.0.0.3(4687). This vulnerability affects the function formApPortalAccessCodeAuth of the file /goform/apPortalAccessCodeAuth. The manipulation of the argument	N/A	H-TEN-I22-080824/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessCode/data/acceInfo leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7582**		
Out-of-bounds Write	07-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda i22 1.0.0.3(4687). This issue affects the function formApPortalOneKeyAuth of the file /goform/apPortalOneKeyAuth. The manipulation of the argument data leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did	N/A	H-TEN-I22-080824/1609

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID: CVE-2024-7583**		
Vendor: Tendacn					
Product: a301					
Affected Version(s): 2.0					
Out-of-bounds Write	07-Aug-2024	9.8	A vulnerability classified as critical has been found in Tenda A301 15.13.08.12. This affects the function formWifiBasicSet of the file /goform/WifiBasicSet. The manipulation of the argument security leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7581**	N/A	H-TEN-A301-080824/1610
Product: fh1201					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the frmL7ImForm function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42942**	N/A	H-TEN-FH12-080824/1611
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromAddressNat function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42945**	N/A	H-TEN-FH12-080824/1612
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the qos parameter in the fromqossetting function. This vulnerability allows attackers to	N/A	H-TEN-FH12-080824/1613

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42949**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the PPW parameter in the fromWizardHandle function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42953**	N/A	H-TEN-FH12-080824/1614
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromwebExcptypemanFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42954**	N/A	H-TEN-FH12-080824/1615
Vendor: totolink					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: a3002r					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Aug-2024	9.8	TOTOLINK A3002R v4.0.0-B20230531.1404 contains a buffer overflow vulnerability in /bin/boa via formParentControl. **CVE ID: CVE-2024-42520**	N/A	H-TOT-A300-080824/1616
Product: a3100r					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Aug-2024	9.8	TOTOLINK A3100R V4.1.2cu.5050_B20200504 has a buffer overflow vulnerability in the password parameter in the loginauth function. **CVE ID: CVE-2024-42546**	N/A	H-TOT-A310-080824/1617
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Aug-2024	9.8	TOTOLINK A3100R V4.1.2cu.5050_B20200504 has a buffer overflow vulnerability in the http_host parameter in the loginauth function. **CVE ID: CVE-2024-42547**	N/A	H-TOT-A310-080824/1618
Product: a3700r					
Affected Version(s): -					
Buffer Copy without Checking	12-Aug-2024	9.8	TOTOLINK A3700R v9.1.2u.5822_B20200513 has a buffer overflow	N/A	H-TOT-A370-080824/1619

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			vulnerability in the http_host parameter in the loginauth function. **CVE ID: CVE-2024-42543**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Aug-2024	9.8	TOTOLINK A3700R v9.1.2u.5822_B20200513 has a buffer overflow vulnerability in the ssid parameter in setWizardCfg function. **CVE ID: CVE-2024-42545**	N/A	H-TOT-A370-080824/1620
Product: cp450					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in TOTOLINK CP450 4.1.0cu.747_B20191224. Affected is the function loginauth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument http_host leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-273558 is the identifier assigned to this	N/A	H-TOT-CP45-080824/1621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7465**		
Product: cp900					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2024	9.8	A vulnerability classified as critical was found in TOTOLINK CP900 6.3c.566. This vulnerability affects the function UploadCustomModule of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument File leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273556. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7463**	N/A	H-TOT-CP90-080824/1622

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in TOTOLINK CP900 6.3c.566. This issue affects the function setTelnetCfg of the component Telnet Service. The manipulation of the argument telnet_enabled leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273557 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7464**	N/A	H-TOT-CP90-080824/1623
Product: lr350					
Affected Version(s): -					
N/A	15-Aug-2024	9.8	Incorrect access control in TOTOLINK LR350 V9.3.5u.6369_B20220309 allows attackers to obtain the apmib configuration file,	N/A	H-TOT-LR35-080824/1624

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which contains the username and the password, via a crafted request to /cgi-bin/ExportSettings.sh. **CVE ID: CVE-2024-42967**		
Product: n350rt					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2024	9.8	A vulnerability classified as critical has been found in TOTOLINK N350RT 9.3.5u.6139_B20201216. This affects the function setWizardCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ssid leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273555. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	H-TOT-N350-080824/1625

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7462		
N/A	15-Aug-2024	9.8	Incorrect access control in TOTOLINK N350RT V9.3.5u.6139_B20201216 allows attackers to obtain the apmib configuration file, which contains the username and the password, via a crafted request to /cgi-bin/ExportSettings.sh. **CVE ID: CVE-2024-42966**	N/A	H-TOT-N350-080824/1626
Product: x5000r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setL2tpServerCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42741**	N/A	H-TOT-X500-080824/1627
Improper Neutralization of Special Elements	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi	N/A	H-TOT-X500-080824/1628

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			contains an OS command injection vulnerability in setUrlFilterRules. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42742**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setSyslogCfg . Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42743**	N/A	H-TOT-X500-080824/1629
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setModifyVpnUser. Authenticated Attackers can send malicious packet to execute arbitrary commands.	N/A	H-TOT-X500-080824/1630

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42744		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setUPnPCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42745**	N/A	H-TOT-X500-080824/1631
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setWanIeCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42747**	N/A	H-TOT-X500-080824/1632
Improper Neutralization of Special Elements used in an OS Command	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in	N/A	H-TOT-X500-080824/1633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			setWiFiWpsCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42748**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	13-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in delBlacklist. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42737**	N/A	H-TOT-X500-080824/1634
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	13-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setDmzCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42738**	N/A	H-TOT-X500-080824/1635
Improper Neutralizat	13-Aug-2024	8.8	In TOTOLINK X5000r	N/A	H-TOT-X500-080824/1636

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setAccessDeviceCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42739**		
Vendor: Vivotek					
Product: cc8160					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Vivotek CC8160 VVTK-0100d and classified as critical. Affected by this issue is the function read of the component httpd. The manipulation of the argument Content-Length leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is	N/A	H-VIV-CC81-080824/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-273524. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the affected release tree is end-of-life. **CVE ID: CVE-2024-7439**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Vivotek CC8160 VVTK-0100d. It has been classified as critical. This affects the function getenv of the file upload_file.cgi. The manipulation of the argument QUERY_STRING leads to command injection. It is possible to initiate the attack remotely. The identifier VDB-273525 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	N/A	H-VIV-CC81-080824/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the affected release tree is end-of-life. **CVE ID: CVE-2024-7440**		
Product: ib8367a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical has been found in Vivotek IB8367A VVTK-0100b. Affected is the function getenv of the file upload_file.cgi. The manipulation of the argument QUERY_STRING leads to command injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-273528. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the affected release tree is end-of-life.	N/A	H-VIV-IB83-080824/1639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7443		
Product: sd9364					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Vivotek SD9364 VVTK-0103f. It has been declared as critical. This vulnerability affects the function read of the component httpd. The manipulation of the argument Content-Length leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273526 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the affected release tree is end-of-life.	N/A	H-VIV-SD93-080824/1640

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7441		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Vivotek SD9364 VVTK-0103f. It has been rated as critical. This issue affects the function getenv of the file upload_file.cgi. The manipulation of the argument QUERY_STRING leads to command injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-273527. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the affected release tree is end-of-life. **CVE ID: CVE-2024-7442**	N/A	H-VIV-SD93-080824/1641
Vendor: vonets					
Product: vap11ac					
Affected Version(s): -					
Improper Neutralizat	12-Aug-2024	9.9	Multiple OS command injection	N/A	H-VON-VAP1-080824/1642

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**		
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**	N/A	H-VON-VAP1-080824/1643

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	H-VON-VAP1-080824/1644
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions	N/A	H-VON-VAP1-080824/1645

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	H-VON-VAP1-080824/1646
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability	N/A	H-VON-VAP1-080824/1647

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	H-VON-VAP1-080824/1648
Product: vap11g					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	H-VON-VAP1-080824/1649
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled.	N/A	H-VON-VAP1-080824/1650

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41161		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	H-VON-VAP1-080824/1651
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge	N/A	H-VON-VAP1-080824/1652

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	H-VON-VAP1-080824/1653
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional	N/A	H-VON-VAP1-080824/1654

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	H-VON-VAP1-080824/1655

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: vap11g-300					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	H-VON-VAP1-080824/1656
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These	N/A	H-VON-VAP1-080824/1657

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	H-VON-VAP1-080824/1658
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets	N/A	H-VON-VAP1-080824/1659

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	H-VON-VAP1-080824/1660

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	H-VON-VAP1-080824/1661
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary	N/A	H-VON-VAP1-080824/1662

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files and bypass authentication. **CVE ID: CVE-2024-41936**		
Product: vap11g-500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	H-VON-VAP1-080824/1663
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication	N/A	H-VON-VAP1-080824/1664

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	H-VON-VAP1-080824/1665
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets	N/A	H-VON-VAP1-080824/1666

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints.	N/A	H-VON-VAP1-080824/1667

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-29082		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	H-VON-VAP1-080824/1668
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated	N/A	H-VON-VAP1-080824/1669

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**		
Product: vap11g-500s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	H-VON-VAP1-080824/1670
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to	N/A	H-VON-VAP1-080824/1671

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	H-VON-VAP1-080824/1672
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets	N/A	H-VON-VAP1-080824/1673

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via	N/A	H-VON-VAP1-080824/1674

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	H-VON-VAP1-080824/1675
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9	N/A	H-VON-VAP1-080824/1676

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**		
Product: vap11n-300					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	H-VON-VAP1-080824/1677
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an	N/A	H-VON-VAP1-080824/1678

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	H-VON-VAP1-080824/1679
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets	N/A	H-VON-VAP1-080824/1680

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass	N/A	H-VON-VAP1-080824/1681

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	H-VON-VAP1-080824/1682
Improper Limitation of a Pathname to a Restricted	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and	N/A	H-VON-VAP1-080824/1683

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**		
Product: vap11s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	H-VON-VAP1-080824/1684
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge	N/A	H-VON-VAP1-080824/1685

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	H-VON-VAP1-080824/1686
Direct Request	12-Aug-2024	9.8	An improper authentication	N/A	H-VON-VAP1-080824/1687

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Forced Browsing')			vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated	N/A	H-VON-VAP1-080824/1688

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	H-VON-VAP1-080824/1689
Improper Limitation of a Pathname	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets	N/A	H-VON-VAP1-080824/1690

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**		
Product: vap11s-5g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	H-VON-VAP1-080824/1691
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and	N/A	H-VON-VAP1-080824/1692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	H-VON-VAP1-080824/1693

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**	N/A	H-VON-VAP1-080824/1694
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9	N/A	H-VON-VAP1-080824/1695

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	H-VON-VAP1-080824/1696

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	H-VON-VAP1-080824/1697
Product: var11n-300					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	H-VON-VAR1-080824/1698
Use of Hard-	08-Aug-2024	9.8	Use of hard-coded credentials	N/A	H-VON-VAR1-080824/1699

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to	N/A	H-VON-VAR1-080824/1700

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code. **CVE ID: CVE-2024-39791**		
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**	N/A	H-VON-VAR1-080824/1701
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets	N/A	H-VON-VAR1-080824/1702

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication	N/A	H-VON-VAR1-080824/1703

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	H-VON-VAR1-080824/1704
Product: var1200-h					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters.	N/A	H-VON-VAR1-080824/1705

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-37023		
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**	N/A	H-VON-VAR1-080824/1706
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an	N/A	H-VON-VAR1-080824/1707

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**		
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**	N/A	H-VON-VAR1-080824/1708
Improper Access Control	12-Aug-2024	8.6	Improper access control	N/A	H-VON-VAR1-080824/1709

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of	N/A	H-VON-VAR1-080824/1710

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	H-VON-VAR1-080824/1711
Product: var1200-l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker	N/A	H-VON-VAR1-080824/1712

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**		
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**	N/A	H-VON-VAR1-080824/1713
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge	N/A	H-VON-VAR1-080824/1714

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**		
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session.	N/A	H-VON-VAR1-080824/1715

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42001		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	H-VON-VAR1-080824/1716
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9	N/A	H-VON-VAR1-080824/1717

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	H-VON-VAR1-080824/1718
Product: var600-h					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software	N/A	H-VON-VAR6-080824/1719

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**		
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**	N/A	H-VON-VAR6-080824/1720
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets	N/A	H-VON-VAR6-080824/1721

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**		
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when	N/A	H-VON-VAR6-080824/1722

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	H-VON-VAR6-080824/1723
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software	N/A	H-VON-VAR6-080824/1724

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	H-VON-VAR6-080824/1725
Product: vbg1200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and	N/A	H-VON-VBG1-080824/1726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**		
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**	N/A	H-VON-VBG1-080824/1727
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets	N/A	H-VON-VBG1-080824/1728

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**		
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a	N/A	H-VON-VBG1-080824/1729

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	H-VON-VBG1-080824/1730
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets	N/A	H-VON-VBG1-080824/1731

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	H-VON-VBG1-080824/1732
Product: vga-1000					
Affected Version(s): -					
Improper Neutralization of Special Elements	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets	N/A	H-VON-VGA--080824/1733

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**		
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**	N/A	H-VON-VGA--080824/1734
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow	N/A	H-VON-VGA--080824/1735

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**		
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an	N/A	H-VON-VGA--080824/1736

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	H-VON-VGA--080824/1737
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets	N/A	H-VON-VGA--080824/1738

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	H-VON-VGA--080824/1739
Vendor: ZTE					
Product: zxv10_et301					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): *					
N/A	08-Aug-2024	8.8	There is a permission and access control vulnerability of ZTE's ZXV10 XT802/ET301 product.Attackers with common permissions can log in the terminal web and change the password of the administrator illegally by intercepting requests to change the passwords. **CVE ID: CVE-2024-22069**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1036424	H-ZTE-ZXV1-080824/1740
Product: zxv10_xt802					
Affected Version(s): *					
N/A	08-Aug-2024	8.8	There is a permission and access control vulnerability of ZTE's ZXV10 XT802/ET301 product.Attackers with common permissions can log in the terminal web and change the password of the administrator illegally by intercepting requests to change the passwords. **CVE ID: CVE-2024-22069**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1036424	H-ZTE-ZXV1-080824/1741

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operating System					
Vendor: airveda					
Product: pm2.5_pm10_monitor_firmware					
Affected Version(s): * Up to (excluding) 7.4.4.39					
Cleartext Transmission of Sensitive Information	12-Aug-2024	6.5	This vulnerability exists in Airveda Air Quality Monitor PM2.5 PM10 due to transmission of sensitive information in plain text during AP pairing mode. An attacker in close proximity could exploit this vulnerability by capturing Wi-Fi traffic of Airveda-AP. Successful exploitation of this vulnerability could allow the attacker to cause Evil Twin attack on the targeted system. **CVE ID: CVE-2024-7408**	N/A	O-AIR-PM2.-080824/1742
Vendor: alientechnology					
Product: alr-f800_firmware					
Affected Version(s): * Up to (including) 19.10.24.00					
Improper Neutralization of Special Elements used in an OS	07-Aug-2024	9.8	A vulnerability was found in Alien Technology ALR-F800 up to 19.10.24.00. It has been rated as critical. Affected by	N/A	O-ALI-ALR--080824/1743

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			this issue is some unknown functionality of the file /admin/system.html. The manipulation of the argument uploadedFile with the input ;whoami leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7580**		
Vendor: annke					
Product: crater_2_firmware					
Affected Version(s): 5.4.1.221222153318					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	8.8	An OS command injection vulnerability in the ccm_debug component of MIPC Camera firmware prior to v5.4.1.240424171021 allows attackers within the same network to execute arbitrary code via a	N/A	O-ANN-CRAT-080824/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTML request. **CVE ID: CVE-2024-39091**		
Vendor: Apple					
Product: iphone_os					
Affected Version(s): -					
Use After Free	06-Aug-2024	8.8	Use after free in Downloads in Google Chrome on iOS prior to 127.0.6533.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-6988**	N/A	O-APP-IPHO-080824/1745
Use After Free	06-Aug-2024	8.8	Use after free in Sharing in Google Chrome on iOS prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7533**	N/A	O-APP-IPHO-080824/1746
Product: macos					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	14-Aug-2024	7.8	Photoshop Desktop versions 24.7.3, 25.9.1 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34117**	https://helpx.adobe.com/security/products/photoshop/apsb24-49.html	O-APP-MACO-080824/1747
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41850**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1748
Out-of-bounds Write	14-Aug-2024	7.8	Illustrator versions 28.5, 27.9.4 and earlier are affected by an out-of-bounds write vulnerability that	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-APP-MACO-080824/1749

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34133**		
Out-of-bounds Write	14-Aug-2024	7.8	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41840**	https://helpx.adobe.com/security/products/bridge/apsb24-59.html	O-APP-MACO-080824/1750
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-080824/1751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41831**		
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41830**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-080824/1752
Out-of-bounds Read	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-080824/1753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39426**		
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39424**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-080824/1754
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-080824/1755

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39383**		
Out-of-bounds Write	14-Aug-2024	7.8	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39386**	https://helpx.adobe.com/security/products/bridge/apsb24-59.html	O-APP-MACO-080824/1756
Out-of-bounds Write	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds write vulnerability that could result in	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-080824/1757

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-2024-39423**		
Use After Free	14-Aug-2024	7.8	Substance3D - Stager versions 3.0.2 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-2024-39388**	N/A	O-APP-MACO-080824/1758
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1759

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39389**		
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-39390**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1760
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-39391**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1761

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39393**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1762
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-39394**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1763

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39422**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-080824/1764
Integer Overflow or Wraparound	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41851**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1765

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41852**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1766
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41853**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1767
N/A	14-Aug-2024	7.8	Illustrator versions 28.5, 27.9.4 and earlier are affected by an Improper Input Validation	https://helpx.adobe.com/security/products/ill	O-APP-MACO-080824/1768

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

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-2024-41856**	ustrator/apsb24-45.html	
Out-of-bounds Read	14-Aug-2024	7.1	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-34127**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1769
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-080824/1770

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(TOCTOU) Race Condition vulnerability that could result in arbitrary code execution in the context of the current user. This issue occurs when the state of a resource changes between its check-time and use-time, allowing an attacker to manipulate the resource. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39420**		
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to privilege escalation. Exploitation of this issue require local low-privilege access to the	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-080824/1771

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected system and attack complexity is high. **CVE ID: CVE-2024-39425**		
NULL Pointer Dereference	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34136**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-APP-MACO-080824/1772
Out-of-bounds Read	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-APP-MACO-080824/1773

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34135**		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41832**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-080824/1774
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability that could lead to	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-080824/1775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41833**		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41834**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-080824/1776
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965,	https://helpx.adobe.com/security/products/ac	O-APP-MACO-080824/1777

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			24.002.20964, 24.001.30123 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-2024-41835**	robat/apsb24-57.html	
Out-of-bounds Read	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 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-2024-34134**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-APP-MACO-080824/1778

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by an Improper Input Validation vulnerability that could lead to an application denial-of-service condition. An attacker could exploit this vulnerability to render the application unresponsive or terminate its execution. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34118**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-APP-MACO-080824/1779
Out-of-bounds Read	14-Aug-2024	5.5	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/bridge/apsb24-59.html	O-APP-MACO-080824/1780

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-39387**		
NULL Pointer Dereference	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34138**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-APP-MACO-080824/1781
NULL Pointer Dereference	14-Aug-2024	5.5	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application,	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1782

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39395**		
Out-of-bounds Read	14-Aug-2024	5.5	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41854**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1783
NULL Pointer Dereference	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS) condition. An attacker could exploit this vulnerability to	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-APP-MACO-080824/1784

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash the application, resulting in a DoS. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34137**		
NULL Pointer Dereference	14-Aug-2024	5.5	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41866**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-APP-MACO-080824/1785
Vendor: Arubanetworks					
Product: arubaos					
Affected Version(s): From (including) 10.3.0.0 Up to (excluding) 10.4.1.4					
Out-of-bounds Write	06-Aug-2024	9.8	There are vulnerabilities in the Soft AP Daemon Service which could	https://support.hpe.com/hpesc/public/docDisplay?docId=hpe	O-ARU-ARUB-080824/1786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a threat actor to execute an unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-42393**	sbnw04678en_us&docLocale=en_US	
Out-of-bounds Write	06-Aug-2024	9.8	There are vulnerabilities in the Soft AP Daemon Service which could allow a threat actor to execute an unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-42394**	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US	O-ARU-ARUB-080824/1787
Out-of-bounds Write	06-Aug-2024	9.8	There is a vulnerability in the AP Certificate Management Service which could allow a threat actor to execute an	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_	O-ARU-ARUB-080824/1788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-42395**	us&docLocale=en_US	
Affected Version(s): From (including) 10.5.0.0 Up to (excluding) 10.6.0.1					
Out-of-bounds Write	06-Aug-2024	9.8	There are vulnerabilities in the Soft AP Daemon Service which could allow a threat actor to execute an unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-42393**	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US	O-ARU-ARUB-080824/1789
Out-of-bounds Write	06-Aug-2024	9.8	There are vulnerabilities in the Soft AP Daemon Service which could allow a threat actor to execute an unauthenticated	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US	O-ARU-ARUB-080824/1790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-42394**		
Out-of-bounds Write	06-Aug-2024	9.8	There is a vulnerability in the AP Certificate Management Service which could allow a threat actor to execute an unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-42395**	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US	O-ARU-ARUB-080824/1791
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 12.0					
Improper Limitation of a Pathname to a	07-Aug-2024	8.8	Attacker controlled files can be uploaded to arbitrary locations on the web server's	N/A	O-DEB-DEBI-080824/1792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			filesystem by abusing a path traversal vulnerability. **CVE ID: CVE-2024-6707**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2024	6.1	Attackers can craft a malicious prompt that coerces the language model into executing arbitrary JavaScript in the context of the web page. **CVE ID: CVE-2024-6706**	N/A	O-DEB-DEBI-080824/1793
Vendor: Dlink					
Product: di-8100_firmware					
Affected Version(s): 16.07					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	15-Aug-2024	9.8	A vulnerability was found in D-Link DI-8100 16.07. It has been classified as critical. This affects the function upgrade_filter_asp of the file upgrade_filter.asp. The manipulation of the argument path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7833**	N/A	O-DLI-DI-8-080824/1794

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dir-300_firmware					
Affected Version(s): 1.06b05_ww					
Use of Hard-coded Credentials	06-Aug-2024	9.8	D-Link DIR-300 REVA FIRMWARE v1.06B05_WW contains hardcoded credentials in the Telnet service. **CVE ID: CVE-2024-41616**	N/A	O-DLI-DIR--080824/1795
Product: dnr-202l_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1796

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function	https://support.announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326,	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1798

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1800

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dnr-322l_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://support.announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1801

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1802

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1803

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1805

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dnr-326_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1806

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1807

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1808

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--080824/1810

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-1100-4_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1811

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1812

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1813

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1815

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-1200-05_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://support.announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1816

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1817

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1818

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1820

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-120_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1821

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1822

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1823

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1825

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-1550-04_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1826

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1827

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1828

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1830

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-315l_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1831

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1832

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1833

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1835

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-320lw_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1837

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1838

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1840

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-320l_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1841

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1842

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1843

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1845

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-320_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1846

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1847

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1848

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-321_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://support.announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1851

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1852

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1853

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1855

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-323_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1856

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1857

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1858

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1860

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-325_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1861

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1862

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1863

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1865

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-326_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1866

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1867

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1868

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1870

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-327l_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1871

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1872

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1873

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1875

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-340l_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1876

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1877

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1878

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1880

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-343_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1881

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1882

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1883

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1885

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-345_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://support.announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1887

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1888

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1890

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Product: dns-726-4_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1891

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1892

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7829**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://support announcement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1893

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7830**		
Buffer Copy without Checking Size of Input ('Classic	15-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7831		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-Aug-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--080824/1895

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7832**		
Vendor: Edimax					
Product: ic-5150w_firmware					
Affected Version(s): * Up to (including) 3.06					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.8	A vulnerability was found in Edimax IC-6220DC and IC-5150W up to 3.06. It has been rated as critical. Affected by this issue is the function cgiFormString of the file ipcam_cgi. The manipulation of the argument host leads to command injection. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7616**	N/A	O-EDI-IC-5-080824/1896
Product: ic-6220dc_firmware					
Affected Version(s): * Up to (including) 3.06					
Improper Neutralization of Special	12-Aug-2024	9.8	A vulnerability was found in Edimax IC-6220DC and IC-5150W up to 3.06.	N/A	O-EDI-IC-6-080824/1897

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			It has been rated as critical. Affected by this issue is the function cgiFormString of the file ipcam_cgi. The manipulation of the argument host leads to command injection. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7616**		
Vendor: Freebsd					
Product: freebsd					
Affected Version(s): * Up to (excluding) 13.0					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Aug-2024	8.1	A signal handler in sshd(8) may call a logging function that is not async-signal-safe. The signal handler is invoked when a client does not authenticate within the LoginGraceTime seconds (120 by default). This signal handler executes in the context of the sshd(8)'s privileged code, which is not sandboxed and	https://security.freebsd.org/advisories/FreeBSD-SA-24:08.openssh.asc	O-FRE-FREE-080824/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			runs with full root privileges. This issue is another instance of the problem in CVE-2024-6387 addressed by FreeBSD-SA-24:04.openssh. The faulty code in this case is from the integration of blacklistd in OpenSSH in FreeBSD. As a result of calling functions that are not async-signal-safe in the privileged sshd(8) context, a race condition exists that a determined attacker may be able to exploit to allow an unauthenticated remote code execution as root. **CVE ID: CVE-2024-7589**		
N/A	12-Aug-2024	7.5	A logic bug in the code which disables kernel tracing for setuid programs meant that tracing was not disabled when it should have, allowing	https://security.freebsd.org/advisories/FreeBSD-SA-24:06.ktrace.asc	O-FRE-FREE-080824/1899

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unprivileged users to trace and inspect the behavior of setuid programs. The bug may be used by an unprivileged user to read the contents of files to which they would not otherwise have access, such as the local password database. **CVE ID: CVE-2024-6760**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	5.3	When mounting a remote filesystem using NFS, the kernel did not sanitize remotely provided filenames for the path separator character, "/". This allows readdir(3) and related functions to return filesystem entries with names containing additional path components. The lack of validation described above gives rise to a confused deputy problem. For example, a program	https://security.freebsd.org/advisories/FreeBSD-SA-24:07.nfsclient.asc	O-FRE-FREE-080824/1900

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			copying files from an NFS mount could be tricked into copying from outside the intended source directory, and/or to a location outside the intended destination directory. **CVE ID: CVE-2024-6759**		
Affected Version(s): 13.3					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Aug-2024	8.1	A signal handler in sshd(8) may call a logging function that is not async-signal-safe. The signal handler is invoked when a client does not authenticate within the LoginGraceTime seconds (120 by default). This signal handler executes in the context of the sshd(8)'s privileged code, which is not sandboxed and runs with full root privileges. This issue is another instance of the problem in CVE-2024-6387	https://security.freebsd.org/advisories/FreeBSD-SA-24:08.openssh.asc	O-FRE-FREE-080824/1901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addressed by FreeBSD-SA-24:04.openssh. The faulty code in this case is from the integration of blacklistd in OpenSSH in FreeBSD. As a result of calling functions that are not async-signal-safe in the privileged sshd(8) context, a race condition exists that a determined attacker may be able to exploit to allow an unauthenticated remote code execution as root. **CVE ID: CVE-2024-7589**		
N/A	12-Aug-2024	7.5	A logic bug in the code which disables kernel tracing for setuid programs meant that tracing was not disabled when it should have, allowing unprivileged users to trace and inspect the behavior of setuid programs. The bug may be used by an	https://security.freebsd.org/advisories/FreeBSD-SA-24:06.ktrace.asc	O-FRE-FREE-080824/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unprivileged user to read the contents of files to which they would not otherwise have access, such as the local password database. **CVE ID: CVE-2024-6760**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	5.3	When mounting a remote filesystem using NFS, the kernel did not sanitize remotely provided filenames for the path separator character, "/". This allows readdir(3) and related functions to return filesystem entries with names containing additional path components. The lack of validation described above gives rise to a confused deputy problem. For example, a program copying files from an NFS mount could be tricked into copying from outside the intended source directory, and/or to a location	https://security.freebsd.org/advisories/FreeBSD-SA-24:07.nfsclient.asc	O-FRE-FREE-080824/1903

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			outside the intended destination directory. **CVE ID: CVE-2024-6759**		
Affected Version(s): 14.0					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Aug-2024	8.1	A signal handler in sshd(8) may call a logging function that is not async-signal-safe. The signal handler is invoked when a client does not authenticate within the LoginGraceTime seconds (120 by default). This signal handler executes in the context of the sshd(8)'s privileged code, which is not sandboxed and runs with full root privileges. This issue is another instance of the problem in CVE-2024-6387 addressed by FreeBSD-SA-24:04.openssh. The faulty code in this case is from the integration of blacklistd in	https://security.freebsd.org/advisories/FreeBSD-SA-24:08.openssh.asc	O-FRE-FREE-080824/1904

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OpenSSH in FreeBSD. As a result of calling functions that are not async-signal-safe in the privileged sshd(8) context, a race condition exists that a determined attacker may be able to exploit to allow an unauthenticated remote code execution as root. **CVE ID: CVE-2024-7589**		
N/A	12-Aug-2024	7.5	A logic bug in the code which disables kernel tracing for setuid programs meant that tracing was not disabled when it should have, allowing unprivileged users to trace and inspect the behavior of setuid programs. The bug may be used by an unprivileged user to read the contents of files to which they would not otherwise have access, such as the	https://security.freebsd.org/advisories/FreeBSD-SA-24:06.ktrace.asc	O-FRE-FREE-080824/1905

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local password database. **CVE ID: CVE-2024-6760**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	5.3	When mounting a remote filesystem using NFS, the kernel did not sanitize remotely provided filenames for the path separator character, "/". This allows readdir(3) and related functions to return filesystem entries with names containing additional path components. The lack of validation described above gives rise to a confused deputy problem. For example, a program copying files from an NFS mount could be tricked into copying from outside the intended source directory, and/or to a location outside the intended destination directory.	https://security.freebsd.org/advisories/FreeBSD-SA-24:07.nfsclient.asc	O-FRE-FREE-080824/1906

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-6759		
Affected Version(s): 14.1					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Aug-2024	8.1	A signal handler in sshd(8) may call a logging function that is not async-signal-safe. The signal handler is invoked when a client does not authenticate within the LoginGraceTime seconds (120 by default). This signal handler executes in the context of the sshd(8)'s privileged code, which is not sandboxed and runs with full root privileges. This issue is another instance of the problem in CVE-2024-6387 addressed by FreeBSD-SA-24:04.openssh. The faulty code in this case is from the integration of blacklistd in OpenSSH in FreeBSD. As a result of calling functions that are	https://security.freebsd.org/advisories/FreeBSD-SA-24:08.openssh.asc	O-FRE-FREE-080824/1907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not async-signal-safe in the privileged sshd(8) context, a race condition exists that a determined attacker may be able to exploit to allow an unauthenticated remote code execution as root. **CVE ID: CVE-2024-7589**		
N/A	12-Aug-2024	7.5	A logic bug in the code which disables kernel tracing for setuid programs meant that tracing was not disabled when it should have, allowing unprivileged users to trace and inspect the behavior of setuid programs. The bug may be used by an unprivileged user to read the contents of files to which they would not otherwise have access, such as the local password database. **CVE ID: CVE-2024-6760**	https://security.freebsd.org/advisories/FreeBSD-SA-24:06.ktrace.asc	O-FRE-FREE-080824/1908
Improper Limitation	12-Aug-2024	5.3	When mounting a remote filesystem	https://security.freebsd.org/ad	O-FRE-FREE-080824/1909

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			using NFS, the kernel did not sanitize remotely provided filenames for the path separator character, "/". This allows readdir(3) and related functions to return filesystem entries with names containing additional path components. The lack of validation described above gives rise to a confused deputy problem. For example, a program copying files from an NFS mount could be tricked into copying from outside the intended source directory, and/or to a location outside the intended destination directory. **CVE ID: CVE-2024-6759**	visories/FreeBSD-SA-24:07.nfsclient.asc	
Affected Version(s): From (including) 13.1 Up to (excluding) 13.3					
Concurrent Execution using Shared	12-Aug-2024	8.1	A signal handler in sshd(8) may call a logging function that is not async-	https://security.freebsd.org/advisories/FreeBSD-SA-	O-FRE-FREE-080824/1910

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			signal-safe. The signal handler is invoked when a client does not authenticate within the LoginGraceTime seconds (120 by default). This signal handler executes in the context of the sshd(8)'s privileged code, which is not sandboxed and runs with full root privileges. This issue is another instance of the problem in CVE-2024-6387 addressed by FreeBSD-SA-24:04.openssh. The faulty code in this case is from the integration of blacklistd in OpenSSH in FreeBSD. As a result of calling functions that are not async-signal-safe in the privileged sshd(8) context, a race condition exists that a determined attacker may be able to exploit to	24:08.openssh.asc	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated remote code execution as root. **CVE ID: CVE-2024-7589**		
N/A	12-Aug-2024	7.5	A logic bug in the code which disables kernel tracing for setuid programs meant that tracing was not disabled when it should have, allowing unprivileged users to trace and inspect the behavior of setuid programs. The bug may be used by an unprivileged user to read the contents of files to which they would not otherwise have access, such as the local password database. **CVE ID: CVE-2024-6760**	https://security.freebsd.org/advisories/FreeBSD-SA-24:06.ktrace.asc	O-FRE-FREE-080824/1911
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	5.3	When mounting a remote filesystem using NFS, the kernel did not sanitize remotely provided filenames for the path separator character, "/". This allows readdir(3)	https://security.freebsd.org/advisories/FreeBSD-SA-24:07.nfsclient.asc	O-FRE-FREE-080824/1912

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and related functions to return filesystem entries with names containing additional path components. The lack of validation described above gives rise to a confused deputy problem. For example, a program copying files from an NFS mount could be tricked into copying from outside the intended source directory, and/or to a location outside the intended destination directory. **CVE ID: CVE-2024-6759**		
Vendor: gl-inet					
Product: a1300_firmware					
Affected Version(s): 4.5.16					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B	N/A	O-GL--A130-080824/1913

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	O-GL--A130-080824/1914

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	O-GL--A130-080824/1915
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000	N/A	O-GL--A130-080824/1916

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-	N/A	O-GL--A130-080824/1917

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: ap1300_firmware					
Affected Version(s): 3.217					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--AP13-080824/1918
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300	N/A	O-GL--AP13-080824/1919

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config.	N/A	O-GL--AP13-080824/1920

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39228		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	O-GL--AP13-080824/1921
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11,	N/A	O-GL--AP13-080824/1922

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/M V1000W/USB150/ N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: ar300m16_firmware					
Affected Version(s): 4.3.11					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were	N/A	O-GL--AR30-080824/1923

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	O-GL--AR30-080824/1924
Improper Neutralization of Special Elements used in an OS Command ('OS	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	O-GL--AR30-080824/1925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated	N/A	O-GL--AR30-080824/1926

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	O-GL--AR30-080824/1927
Product: ar300m_firmware					
Affected Version(s): 4.3.11					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--AR30-080824/1928
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be	N/A	O-GL--AR30-080824/1929

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	O-GL--AR30-080824/1930
Improper Neutralization of Special Elements in Output Used by a Downstrea	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/	N/A	O-GL--AR30-080824/1931

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and	N/A	O-GL--AR30-080824/1932

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: ar750s_firmware					
Affected Version(s): 4.3.11					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--AR75-080824/1933
Improper Limitation of a	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M1	N/A	O-GL--AR75-080824/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			6/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to	N/A	O-GL--AR75-080824/1935

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	O-GL--AR75-080824/1936

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	O-GL--AR75-080824/1937
Product: ar750_firmware					
Affected Version(s): 4.3.11					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	O-GL--AR75-080824/1938

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	O-GL--AR75-080824/1939

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	O-GL--AR75-080824/1940
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000	N/A	O-GL--AR75-080824/1941

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-	N/A	O-GL--AR75-080824/1942

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: ax1800_firmware					
Affected Version(s): 4.5.16					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--AX18-080824/1943
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300	N/A	O-GL--AX18-080824/1944

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config.	N/A	O-GL--AX18-080824/1945

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39228		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	O-GL--AX18-080824/1946
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11,	N/A	O-GL--AX18-080824/1947

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/M V1000W/USB150/ N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: axt1800_firmware					
Affected Version(s): 4.5.16					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were	N/A	O-GL--AXT1-080824/1948

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	O-GL--AXT1-080824/1949
Improper Neutralization of Special Elements used in an OS Command ('OS	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	O-GL--AXT1-080824/1950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated	N/A	O-GL--AXT1-080824/1951

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	O-GL--AXT1-080824/1952
Product: b1300_firmware					
Affected Version(s): 4.3.11					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--B130-080824/1953
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be	N/A	O-GL--B130-080824/1954

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	O-GL--B130-080824/1955
Improper Neutralization of Special Elements in Output Used by a Downstrea	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/	N/A	O-GL--B130-080824/1956

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and	N/A	O-GL--B130-080824/1957

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: b2200_firmware					
Affected Version(s): 3.216					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--B220-080824/1958
Improper Limitation of a	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M1	N/A	O-GL--B220-080824/1959

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			6/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to	N/A	O-GL--B220-080824/1960

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	O-GL--B220-080824/1961

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	O-GL--B220-080824/1962
Product: e750_firmware					
Affected Version(s): 4.3.12					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	O-GL--E750-080824/1963

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	O-GL--E750-080824/1964

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	O-GL--E750-080824/1965
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000	N/A	O-GL--E750-080824/1966

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-	N/A	O-GL--E750-080824/1967

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: mt1300_firmware					
Affected Version(s): 4.3.11					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--MT13-080824/1968
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300	N/A	O-GL--MT13-080824/1969

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config.	N/A	O-GL--MT13-080824/1970

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39228		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	O-GL--MT13-080824/1971
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11,	N/A	O-GL--MT13-080824/1972

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/M V1000W/USB150/ N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: mt2500_firmware					
Affected Version(s): 4.5.16					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were	N/A	O-GL--MT25-080824/1973

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	O-GL--MT25-080824/1974
Improper Neutralization of Special Elements used in an OS Command ('OS	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	O-GL--MT25-080824/1975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated	N/A	O-GL--MT25-080824/1976

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	O-GL--MT25-080824/1977
Product: mt3000_firmware					
Affected Version(s): 4.5.16					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--MT30-080824/1978
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be	N/A	O-GL--MT30-080824/1979

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	O-GL--MT30-080824/1980
Improper Neutralization of Special Elements in Output Used by a Downstrea	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/	N/A	O-GL--MT30-080824/1981

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and	N/A	O-GL--MT30-080824/1982

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: mt300n-v2_firmware					
Affected Version(s): 4.3.11					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--MT30-080824/1983
Improper Limitation of a	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M1	N/A	O-GL--MT30-080824/1984

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			6/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to	N/A	O-GL--MT30-080824/1985

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	O-GL--MT30-080824/1986

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	O-GL--MT30-080824/1987
Product: mt6000_firmware					
Affected Version(s): 4.5.8					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	O-GL--MT60-080824/1988

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	O-GL--MT60-080824/1989

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	O-GL--MT60-080824/1990
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000	N/A	O-GL--MT60-080824/1991

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-	N/A	O-GL--MT60-080824/1992

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: mv1000w_firmware					
Affected Version(s): 3.216					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--MV10-080824/1993
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300	N/A	O-GL--MV10-080824/1994

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config.	N/A	O-GL--MV10-080824/1995

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39228		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	O-GL--MV10-080824/1996
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11,	N/A	O-GL--MV10-080824/1997

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/M V1000W/USB150/ N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: mv1000_firmware					
Affected Version(s): 3.216					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were	N/A	O-GL--MV10-080824/1998

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	O-GL--MV10-080824/1999
Improper Neutralization of Special Elements used in an OS Command ('OS	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	O-GL--MV10-080824/2000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated	N/A	O-GL--MV10-080824/2001

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	O-GL--MV10-080824/2002
Product: n300_firmware					
Affected Version(s): 3.216					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--N300-080824/2003
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be	N/A	O-GL--N300-080824/2004

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	O-GL--N300-080824/2005
Improper Neutralization of Special Elements in Output Used by a Downstrea	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/	N/A	O-GL--N300-080824/2006

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and	N/A	O-GL--N300-080824/2007

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: s1300_firmware					
Affected Version(s): 3.216					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--S130-080824/2008
Improper Limitation of a	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M1	N/A	O-GL--S130-080824/2009

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			6/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to	N/A	O-GL--S130-080824/2010

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	O-GL--S130-080824/2011

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	O-GL--S130-080824/2012
Product: sf1200_firmware					
Affected Version(s): 3.216					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	O-GL--SF12-080824/2013

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	O-GL--SF12-080824/2014

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	O-GL--SF12-080824/2015
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000	N/A	O-GL--SF12-080824/2016

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-	N/A	O-GL--SF12-080824/2017

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: sft1200_firmware					
Affected Version(s): 4.3.11					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--SFT1-080824/2018
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300	N/A	O-GL--SFT1-080824/2019

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config.	N/A	O-GL--SFT1-080824/2020

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39228		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	O-GL--SFT1-080824/2021
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11,	N/A	O-GL--SFT1-080824/2022

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: usb150_firmware					
Affected Version(s): 3.216					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were	N/A	O-GL--USB1-080824/2023

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	O-GL--USB1-080824/2024
Improper Neutralization of Special Elements used in an OS Command ('OS	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	O-GL--USB1-080824/2025

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated	N/A	O-GL--USB1-080824/2026

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	O-GL--USB1-080824/2027
Product: x3000_firmware					
Affected Version(s): 4.4.8					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--X300-080824/2028
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be	N/A	O-GL--X300-080824/2029

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	O-GL--X300-080824/2030
Improper Neutralization of Special Elements in Output Used by a Downstrea	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/	N/A	O-GL--X300-080824/2031

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and	N/A	O-GL--X300-080824/2032

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: x300b_firmware					
Affected Version(s): 4.5.16					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--X300-080824/2033
Improper Limitation of a	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M1	N/A	O-GL--X300-080824/2034

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			6/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to	N/A	O-GL--X300-080824/2035

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	O-GL--X300-080824/2036

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	O-GL--X300-080824/2037
Product: x750_firmware					
Affected Version(s): 4.3.11					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	O-GL--X750-080824/2038

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	O-GL--X750-080824/2039

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**	N/A	O-GL--X750-080824/2040
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000	N/A	O-GL--X750-080824/2041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-	N/A	O-GL--X750-080824/2042

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: xe3000_firmware					
Affected Version(s): 4.4.8					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**	N/A	O-GL--XE30-080824/2043
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300	N/A	O-GL--XE30-080824/2044

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config.	N/A	O-GL--XE30-080824/2045

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39228		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**	N/A	O-GL--XE30-080824/2046
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11,	N/A	O-GL--XE30-080824/2047

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/M V1000W/USB150/ N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**		
Product: xe300_firmware					
Affected Version(s): 4.3.16					
Improper Restriction of Excessive Authentication Attempts	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/A R300M/AR300M1 6/MT300N-V2/B1300/MT130 0/SFT1200/X750 v4.3.11, MT3000/MT2500/ AXT1800/AX1800/ A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were	N/A	O-GL--XE30-080824/2048

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a remote code execution (RCE) vulnerability. **CVE ID: CVE-2024-39225**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a vulnerability can be exploited to manipulate routers by passing malicious shell commands through the s2s API. **CVE ID: CVE-2024-39226**	N/A	O-GL--XE30-080824/2049
Improper Neutralization of Special Elements used in an OS Command ('OS	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/	N/A	O-GL--XE30-080824/2050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain a shell injection vulnerability via the interface check_ovpn_client_config and check_config. **CVE ID: CVE-2024-39228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-2024	9.8	GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4 were discovered to contain insecure permissions in the endpoint /cgi-bin/glc. This vulnerability allows unauthenticated	N/A	O-GL--XE30-080824/2051

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary code or possibly a directory traversal via crafted JSON data. **CVE ID: CVE-2024-39227**		
N/A	06-Aug-2024	5.3	An issue in GL-iNet products AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, XE3000/X3000 v4, and B2200/MV1000/MV1000W/USB150/N300/SF1200 v3.216 allows attackers to intercept communications via a man-in-the-middle attack when DDNS clients are reporting data to the server. **CVE ID: CVE-2024-39229**	N/A	O-GL--XE30-080824/2052
Vendor: gncchome					
Product: gncc_c2_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Hard-coded Credentials	15-Aug-2024	6.8	Identical Hardcoded Root Password for All Devices in GNCC's GC2 Indoor Security Camera 1080P allows an attacker with physical access to retrieve the root password for all similar devices **CVE ID: CVE-2024-31798**	N/A	O-GNC-GNCC-080824/2053
Improper Authentication	15-Aug-2024	6.8	Authentication Bypass in GNCC's GC2 Indoor Security Camera 1080P allows an attacker with physical access to gain a privileged command shell via the UART Debugging Port. **CVE ID: CVE-2024-31800**	N/A	O-GNC-GNCC-080824/2054
Cleartext Transmission of Sensitive Information	15-Aug-2024	4.6	Information Disclosure in GNCC's GC2 Indoor Security Camera 1080P allows an attacker with physical access to read the WiFi passphrase via the UART Debugging Port. **CVE ID: CVE-2024-31799**	N/A	O-GNC-GNCC-080824/2055

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	06-Aug-2024	4.7	Inappropriate implementation in Fullscreen in Google Chrome on Android prior to 127.0.6533.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-6995**	N/A	O-GOO-ANDR-080824/2056
Vendor: hms-networks					
Product: ewon_cosy\+_firmware					
Affected Version(s): From (including) 21.0s0 Up to (excluding) 21.2s10					
Direct Request ('Forced Browsing')	06-Aug-2024	9.1	A compromised HMS Networks Cosy+ device could be used to request a Certificate Signing Request from Talk2m for another device, resulting in an availability issue. The issue was patched on the Talk2m production server on April 18, 2024.	https://hmsnetworks.blob.core.windows.net/nlw/docs/default-source/products/cybersecurity/security-advisory/hms-security-advisory-2024-07-29-001--ewon-several-cosy--vulnerabilities.pdf,	O-HMS-EWON-080824/2057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33897	https://www.hms-networks.com/cyber-security	
Affected Version(s): From (including) 22.0s0 Up to (excluding) 22.1s3					
Direct Request ('Forced Browsing')	06-Aug-2024	9.1	A compromised HMS Networks Cosy+ device could be used to request a Certificate Signing Request from Talk2m for another device, resulting in an availability issue. The issue was patched on the Talk2m production server on April 18, 2024. **CVE ID: CVE-2024-33897**	https://hmsnetworks.blob.core.windows.net/nlw/docs/default-source/products/cybersecurity/security-advisory/hms-security-advisory-2024-07-29-001--ewon-several-cosy--vulnerabilities.pdf, https://www.hms-networks.com/cyber-security	O-HMS-EWON-080824/2058
Vendor: HP					
Product: instantos					
Affected Version(s): From (including) 6.4.0.0 Up to (excluding) 8.10.0.13					
Out-of-bounds Write	06-Aug-2024	9.8	There are vulnerabilities in the Soft AP Daemon Service which could allow a threat actor to execute an unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US	O-HP-INST-080824/2059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system leading to complete system compromise. **CVE ID: CVE-2024-42393**		
Out-of-bounds Write	06-Aug-2024	9.8	There are vulnerabilities in the Soft AP Daemon Service which could allow a threat actor to execute an unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-42394**	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US	O-HP-INST-080824/2060
Out-of-bounds Write	06-Aug-2024	9.8	There is a vulnerability in the AP Certificate Management Service which could allow a threat actor to execute an unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US	O-HP-INST-080824/2061

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system compromise. **CVE ID: CVE-2024-42395**		
Affected Version(s): From (including) 8.12.0.0 Up to (excluding) 8.12.0.2					
Out-of-bounds Write	06-Aug-2024	9.8	There are vulnerabilities in the Soft AP Daemon Service which could allow a threat actor to execute an unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-42393**	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US	O-HP-INST-080824/2062
Out-of-bounds Write	06-Aug-2024	9.8	There are vulnerabilities in the Soft AP Daemon Service which could allow a threat actor to execute an unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US	O-HP-INST-080824/2063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system compromise. **CVE ID: CVE-2024-42394**		
Out-of-bounds Write	06-Aug-2024	9.8	There is a vulnerability in the AP Certificate Management Service which could allow a threat actor to execute an unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-42395**	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US	O-HP-INST-080824/2064
Product: poly_clariti_manager_firmware					
Affected Version(s): * Up to (including) 10.10.2.2					
Unrestricted Upload of File with Dangerous Type	06-Aug-2024	8.8	A vulnerability was discovered in the firmware builds up to 10.10.2.2 in Poly Clariti Manager devices. The firmware flaw does not properly sanitize User input. **CVE ID: CVE-2024-41913**	https://support.hp.com/us-en/document/ish_11006488-11006512-16/hpsbpy03957	O-HP-POLY-080824/2065
Improper Neutralization of Input	06-Aug-2024	6.1	A vulnerability was discovered in the firmware builds up	https://support.hp.com/us-en/document/i	O-HP-POLY-080824/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			to 10.10.2.2 in Poly Clariti Manager devices. The firmware contained multiple XSS vulnerabilities in the version of JavaScript used. **CVE ID: CVE-2024-41910**	sh_11006981-11007005-16/hpsbpy03960	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2024	5.4	A vulnerability was discovered in the firmware builds up to 10.10.2.2 in Poly Clariti Manager devices. The flaw does not properly neutralize input during a web page generation. **CVE ID: CVE-2024-41911**	https://support.hp.com/us-en/document/ish_11006770-11006795-16/hpsbpy03959	O-HP-POLY-080824/2067
Vendor: Huawei					
Product: emui					
Affected Version(s): 12.0.0					
N/A	08-Aug-2024	7.5	Access permission verification vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42031**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-EMUI-080824/2068
N/A	08-Aug-2024	5.5	Access permission verification vulnerability in the Contacts module	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-EMUI-080824/2069

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42032**		
Affected Version(s): 13.0.0					
N/A	08-Aug-2024	7.5	Access permission verification vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42031**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-EMUI-080824/2070
N/A	08-Aug-2024	6.2	Access permission verification vulnerability in the content sharing pop-up module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42030**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-EMUI-080824/2071
N/A	08-Aug-2024	5.5	Access permission verification vulnerability in the Contacts module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-EMUI-080824/2072

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42032		
Affected Version(s): 14.0.0					
N/A	08-Aug-2024	7.5	Access permission verification vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42031**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-EMUI-080824/2073
N/A	08-Aug-2024	6.2	Access permission verification vulnerability in the content sharing pop-up module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42030**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-EMUI-080824/2074
N/A	08-Aug-2024	5.5	Access permission verification vulnerability in the Contacts module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42032**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-EMUI-080824/2075
Product: harmonyos					
Affected Version(s): 2.0.0					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2024	7.5	Access permission verification vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42031**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2076
N/A	08-Aug-2024	5.5	Access permission verification vulnerability in the Contacts module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42032**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2077
Affected Version(s): 2.1.0					
N/A	08-Aug-2024	7.5	Access permission verification vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42031**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2078
N/A	08-Aug-2024	5.5	Access permission verification vulnerability in the Contacts module Impact: Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2079

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42032**		
Affected Version(s): 3.0.0					
N/A	08-Aug-2024	7.5	Access permission verification vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42031**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2080
N/A	08-Aug-2024	5.5	Access permission verification vulnerability in the Contacts module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42032**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2081
Affected Version(s): 3.1.0					
N/A	08-Aug-2024	7.5	Access permission verification vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42031**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2082

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2024	6.2	Access permission verification vulnerability in the content sharing pop-up module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42030**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2083
N/A	08-Aug-2024	5.5	Access permission verification vulnerability in the Contacts module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42032**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2084
Affected Version(s): 4.0.0					
N/A	08-Aug-2024	7.5	Access permission verification vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42031**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2085
N/A	08-Aug-2024	6.2	Access permission verification vulnerability in the content sharing pop-up module	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2086

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42030**		
N/A	08-Aug-2024	5.5	Access permission verification vulnerability in the Contacts module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42032**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2087
Affected Version(s): 4.2.0					
N/A	08-Aug-2024	7.5	Access permission verification vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42031**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2088
N/A	08-Aug-2024	6.2	Access permission verification vulnerability in the content sharing pop-up module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2089

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42030		
N/A	08-Aug-2024	5.5	Access permission verification vulnerability in the Contacts module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42032**	https://consumer.huawei.com/en/support/bulletin/2024/8/	O-HUA-HARM-080824/2090
Vendor: kaongroup					
Product: ar2140_firmware					
Affected Version(s): From (including) 3.2.46 Up to (excluding) 4.2.16					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Aug-2024	7.2	Firmware in KAON AR2140 routers prior to version 4.2.16 is vulnerable to a shell command injection via sending a crafted request to one of the endpoints. In order to exploit this vulnerability, one has to have access to the administrative portal of the router. **CVE ID: CVE-2024-3659**	N/A	O-KAO-AR21-080824/2091
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): * Up to (excluding) 4.19.318					
Use After Free	07-Aug-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/	O-LIN-LINU-080824/2092

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: libceph: fix race between delayed_work() and ceph_monc_stop() The way the delayed work is handled in ceph_monc_stop() is prone to races with mon_fault() and possibly also finish_hunting(). Both of these can requeue the delayed work which wouldn't be canceled by any of the following code in case that happens after cancel_delayed_work_sync() runs -- __close_session() doesn't mess with the delayed work in order to avoid interfering with the hunting interval logic. This part was missed in commit b5d91704f53e	1177afeca833174ba83504688eec898c6214f4bf, https://git.kernel.org/stable/c/20cf67dcb7db842f941eff1af6ee5e9dc41796d7, https://git.kernel.org/stable/c/2d33654d40a05afd91ab24c9a73ab512a0670a9a	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			("libceph: behave in mon_fault() if cur_mon < 0") and use-after-free can still ensue on monc and objects that hang off of it, with monc->auth and monc->monmap being particularly susceptible to quickly being reused. To fix this: - clear monc->cur_mon and monc->hunting as part of closing the session in ceph_monc_stop() - bail from delayed_work() if monc->cur_mon is cleared, similar to how it's done in mon_fault() and finish_hunting() (based on monc->hunting) - call cancel_delayed_work_sync() after the session is closed **CVE ID: CVE-2024-42232**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: configfs: Prevent OOB read/write in usb_string_copy() Userspace provided string 's' could trivially have the length zero. Left unchecked this will firstly result in an OOB read in the form `if (str[0 - 1] == '\n')` followed closely by an OOB write in the form `str[0 - 1] = '\0'`. There is already a validating check to catch strings that are too long. Let's supply an additional check for invalid strings that are too short. **CVE ID: CVE-2024-42236**	https://git.kernel.org/stable/c/2d16f63d8030903e5031853e79d731ee5d474e70, https://git.kernel.org/stable/c/6d3c721e686ea6c59e18289b400cc95c76e927e0, https://git.kernel.org/stable/c/72b8ee0d9826e8ed00e0bdfce3e46b98419b37ce	O-LIN-LINU-080824/2093
Affected Version(s): * Up to (excluding) 5.16					
Excessive Iteration	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/259955eca9b7acf1299b1ac077d8cfbe12df35d	O-LIN-LINU-080824/2094

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware: cs_dsp: Validate payload length before processing block Move the payload length check in cs_dsp_load() and cs_dsp_coeff_load() to be done before the block is processed. The check that the length of a block payload does not exceed the number of remaining bytes in the firwmware file buffer was being done near the end of the loop iteration. However, some code before that check used the length field without validating it. **CVE ID: CVE-2024-42237**	8, https://git.kernel.org/stable/c/3a9cd924aec1288d675df721f244da4dd7e16cff, https://git.kernel.org/stable/c/6598afa9320b6ab13041616950ca5f8f938c0cf1	
Affected Version(s): From (including) 3.3 Up to (excluding) 5.10.222					
N/A	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: USB: serial: mos7840: fix crash on resume	https://git.kernel.org/stable/c/1094ed500987e67a9d18b0f95e1812f1cc720856, https://git.kernel.org/stable/c/553e67dec8463	O-LIN-LINU-080824/2095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Since commit c49cfa917025 ("USB: serial: use generic method if no alternative is provided in usb serial layer"), USB serial core calls the generic resume implementation when the driver has not provided one. This can trigger a crash on resume with mos7840 since support for multiple read URBs was added back in 2011. Specifically, both port read URBs are now submitted on resume for open ports, but the context pointer of the second URB is left set to the core rather than mos7840 port structure. Fix this by implementing dedicated suspend and resume functions for mos7840.	23b5575e78a776cf594c13f98c4, https://git.kernel.org/stable/c/5ae6a64f18211851c8df6b4221381c438b9a7348	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tested with Delock 87414 USB 2.0 to 4x serial adapter. [johan: analyse crash and rewrite commit message; set busy flag on resume; drop bulk-in check; drop unnecessary usb_kill_urb()] **CVE ID: CVE-2024-42244**		
Affected Version(s): From (including) 4.17 Up to (excluding) 6.1.100					
Loop with Unreachable Exit Condition ('Infinite Loop')	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net, sunrpc: Remap EPERM in case of connection failure in xs_tcp_setup_socket When using a BPF program on kernel_connect(), the call can return -EPERM. This causes xs_tcp_setup_socket() to loop forever, filling up the syslog and causing	https://git.kernel.org/stable/c/626dfed5fa3bfb41e0dffd796032b555b69f9cde, https://git.kernel.org/stable/c/d6c686c01c5f12ff8f7264e0ddf71df6cb0d4414, https://git.kernel.org/stable/c/f2431e7db0fe0daccb2f06bb0d23740affcd2fa6	O-LIN-LINU-080824/2096

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the kernel to potentially freeze up. Neil suggested: This will propagate -EPERM up into other layers which might not be ready to handle it. It might be safer to map EPERM to an error we would be more likely to expect from the network system - such as ECONNREFUSED or ENETDOWN. ECONNREFUSED as error seems reasonable. For programs setting a different error can be out of reach (see handling in 4fbac77d2d09) in particular on kernels which do not have f10d05966196 ("bpf: Make BPF_PROG_RUN_ARRAY return -err instead of allow boolean"), thus given that it is		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			better to simply remap for consistent behavior. UDP does handle EPERM in xs_udp_send_request(). **CVE ID: CVE-2024-42246**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.280					
Use After Free	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: libceph: fix race between delayed_work() and ceph_monc_stop() The way the delayed work is handled in ceph_monc_stop() is prone to races with mon_fault() and possibly also finish_hunting(). Both of these can requeue the delayed work which wouldn't be canceled by any of the following code in case that happens after cancel_delayed_work_sync()	https://git.kernel.org/stable/c/1177afeca833174ba83504688eec898c6214f4bf, https://git.kernel.org/stable/c/20cf67dcb7db842f941eff1af6ee5e9dc41796d7, https://git.kernel.org/stable/c/2d33654d40a05afd91ab24c9a73ab512a0670a9a	O-LIN-LINU-080824/2097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			runs --__close_session() doesn't mess with the delayed work in order to avoid interfering with the hunting interval logic. This part was missed in commit b5d91704f53e ("libceph: behave in mon_fault() if cur_mon < 0") and use-after-free can still ensue on monc and objects that hang off of it, with monc->auth and monc->monmap being particularly susceptible to quickly being reused. To fix this: - clear monc->cur_mon and monc->hunting as part of closing the session in ceph_monc_stop() - bail from delayed_work() if monc->cur_mon is cleared, similar to how		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it's done in mon_fault() and finish_hunting() (based on monc->hunting) - call cancel_delayed_work_sync() after the session is closed **CVE ID: CVE-2024-42232**		
Out-of-bounds Write	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: configfs: Prevent OOB read/write in usb_string_copy() Userspace provided string 's' could trivially have the length zero. Left unchecked this will firstly result in an OOB read in the form `if (str[0 - 1] == '\n') followed closely by an OOB write in the form `str[0 - 1] = '\0'`. There is already a validating check to catch strings that are too long.	https://git.kernel.org/stable/c/2d16f63d8030903e5031853e79d731ee5d474e70, https://git.kernel.org/stable/c/6d3c721e686ea6c59e18289b400cc95c76e927e0, https://git.kernel.org/stable/c/72b8ee0d9826e8ed00e0bdfce3e46b98419b37ce	O-LIN-LINU-080824/2098

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Let's supply an additional check for invalid strings that are too short. **CVE ID: CVE-2024-42236**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.163					
Use After Free	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: libceph: fix race between delayed_work() and ceph_monc_stop() The way the delayed work is handled in ceph_monc_stop() is prone to races with mon_fault() and possibly also finish_hunting(). Both of these can requeue the delayed work which wouldn't be canceled by any of the following code in case that happens after cancel_delayed_work_sync() runs -- __close_session() doesn't mess with	https://git.kernel.org/stable/c/1177afeca833174ba83504688eec898c6214f4bf, https://git.kernel.org/stable/c/20cf67dcb7db842f941eff1af6ee5e9dc41796d7, https://git.kernel.org/stable/c/2d33654d40a05afd91ab24c9a73ab512a0670a9a	O-LIN-LINU-080824/2099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the delayed work in order to avoid interfering with the hunting interval logic. This part was missed in commit b5d91704f53e ("libceph: behave in mon_fault() if cur_mon < 0") and use-after-free can still ensue on monc and objects that hang off of it, with monc->auth and monc->monmap being particularly susceptible to quickly being reused. To fix this: - clear monc->cur_mon and monc->hunting as part of closing the session in ceph_monc_stop() - bail from delayed_work() if monc->cur_mon is cleared, similar to how it's done in mon_fault() and finish_hunting()		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(based on monc->hunting) - call cancel_delayed_work_sync() after the session is closed **CVE ID: CVE-2024-42232**		
Out-of-bounds Write	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: configfs: Prevent OOB read/write in usb_string_copy() Userspace provided string 's' could trivially have the length zero. Left unchecked this will firstly result in an OOB read in the form `if (str[0 - 1] == '\n')` followed closely by an OOB write in the form `str[0 - 1] = '\0'`. There is already a validating check to catch strings that are too long. Let's supply an additional check for	https://git.kernel.org/stable/c/2d16f63d8030903e5031853e79d731ee5d474e70, https://git.kernel.org/stable/c/6d3c721e686ea6c59e18289b400cc95c76e927e0, https://git.kernel.org/stable/c/72b8ee0d9826e8ed00e0bdfce3e46b98419b37ce	O-LIN-LINU-080824/2100

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid strings that are too short. **CVE ID: CVE-2024-42236**		
N/A	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: USB: serial: mos7840: fix crash on resume Since commit c49cfa917025 ("USB: serial: use generic method if no alternative is provided in usb serial layer"), USB serial core calls the generic resume implementation when the driver has not provided one. This can trigger a crash on resume with mos7840 since support for multiple read URBs was added back in 2011. Specifically, both port read URBs are now submitted on resume for open ports, but the context pointer	https://git.kernel.org/stable/c/1094ed500987e67a9d18b0f95e1812f1cc720856, https://git.kernel.org/stable/c/553e67dec846323b5575e78a776cf594c13f98c4, https://git.kernel.org/stable/c/5ae6a64f18211851c8df6b4221381c438b9a7348	O-LIN-LINU-080824/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the second URB is left set to the core rather than mos7840 port structure. Fix this by implementing dedicated suspend and resume functions for mos7840. Tested with Delock 87414 USB 2.0 to 4x serial adapter. [johan: analyse crash and rewrite commit message; set busy flag on resume; drop bulk-in check; drop unnecessary usb_kill_urb()] **CVE ID: CVE-2024-42244**		
Allocation of Resources Without Limits or Throttling	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: wireguard: allowedips: avoid unaligned 64-bit memory accesses On the parisc platform, the kernel	https://git.kernel.org/stable/c/217978a29c6ceca76d3c640bf94bdf50c268d801, https://git.kernel.org/stable/c/2fb34bf76431e831f9863cd59adc0bd1f67b0fbf, https://git.kern	O-LIN-LINU-080824/2102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issues kernel warnings because swap_endian() tries to load a 128-bit IPv6 address from an unaligned memory location: Kernel: unaligned access to 0x55f4688c in wg_allowedips_insert_v6+0x2c/0x80 [wireguard] (iir 0xf3010df) Kernel: unaligned access to 0x55f46884 in wg_allowedips_insert_v6+0x38/0x80 [wireguard] (iir 0xf2010dc) Avoid such unaligned memory accesses by instead using the get_unaligned_be64() helper macro. [Jason: replace src[8] in original patch with src+8] **CVE ID: CVE-2024-42247**	el.org/stable/c/6638a203abad35fa636d59ac47bdbc4bc100fd74	
Affected Version(s): From (including) 5.15 Up to (excluding) 6.6.41					
Improper Locking	07-Aug-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/3e4e8178a8666c56813bd167b	O-LIN-LINU-080824/2103

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			vulnerability has been resolved:
			
			bpf: Fail bpf_timer_cancel when callback is being cancelled
			
			Given a schedule:
			
			timer1 cb
			
			timer2 cb
			
			bpf_timer_cancel(timer2);
			bpf_timer_cancel(timer1);
			
			Both bpf_timer_cancel calls would wait for the other callback to finish
			executing, introducing a lockup.
			
			Add an atomic_t count named 'cancelling' in bpf_hrtimer. This keeps
			track of all in-flight cancellation requests for a given BPF timer.
			Whenever cancelling a BPF
				848fca0f4c9af0a, https://git.kernel.org/stable/c/9369830518688ecd5b08ffc08ab3302ce2b5d0f7, https://git.kernel.org/stable/c/d4523831f07a267a943f0dde844bf8ead7495f13	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			timer, we must check if we have outstanding cancellation requests, and if so, we must fail the operation with an error (-EDEADLK) since cancellation is synchronous and waits for the callback to finish executing. This implies that we can enter a deadlock situation involving two or more timer callbacks executing in parallel and attempting to cancel one another. Note that we avoid incrementing the cancelling counter for the target timer (the one being cancelled) if bpf_timer_cancel is not invoked from a callback, to avoid spurious errors. The whole point of detecting cur->cancelling and returning -EDEADLK is to not enter a busy wait loop		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			(which may or may not lead to a lockup). This does not apply in case the
			caller is in a non-callback context, the other side can continue to
			cancel as it sees fit without running into errors.
			
			Background on prior attempts:
			
			Earlier versions of this patch used a bool 'cancelling' bit and used the
			following pattern under timer->lock to publish cancellation status.
			
			lock(t->lock);
			t->cancelling = true;
			mb();
			if (cur->cancelling)
			return -EDEADLK;
			unlock(t->lock);
			hrtimer_cancel(t->timer);
			t->cancelling = false;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The store outside the critical section could overwrite a parallel requests t->cancelling assignment to true, to ensure the parallely executing callback observes its cancellation status. It would be necessary to clear this cancelling bit once hrtimer_cancel is done, but lack of serialization introduced races. Another option was explored where bpf_timer_start would clear the bit when (re)starting the timer under timer->lock. This would ensure serialized access to the cancelling bit, but may allow it to be cleared before in-flight hrtimer_cancel has finished executing, such that lockups can occur again.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thus, we choose an atomic counter to keep track of all outstanding cancellation requests and use it to prevent lockups in case callbacks attempt to cancel each other while executing in parallel. **CVE ID: CVE-2024-42239**		
Affected Version(s): From (including) 5.15.163 Up to (excluding) 6.1.100					
Loop with Unreachable Exit Condition ('Infinite Loop')	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: x86/bhi: Avoid warning in #DB handler due to BHI mitigation When BHI mitigation is enabled, if SYSENTER is invoked with the TF flag set then entry_SYSENTER_compat() uses CLEAR_BRANCH_HISTORY and calls the clear_bhb_loop() before the TF flag is	https://git.kernel.org/stable/c/08518d48e5b744620524f0acd7c26c19bda7f513, https://git.kernel.org/stable/c/a765679defe1dc1b8fa01928a6ad6361e72a1364, https://git.kernel.org/stable/c/ac8b270b61d48fcc61f052097777e3b5e11591e0	O-LIN-LINU-080824/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			cleared. This causes the #DB handler
			(exc_debug_kernel()) to issue a warning because single-step is used outside the
			entry_SYSENTER_compat() function.
			
			To address this issue, entry_SYSENTER_compat() should use CLEAR_BRANCH_HISTORY
			after making sure the TF flag is cleared.
			
			The problem can be reproduced with the following sequence:
			
			$ cat sysenter_step.c
			int main()
			{ asm("pushf; pop %ax; bts $8,%ax; push %ax; popf; sysenter"); }
			
			$ gcc -o sysenter_step sysenter_step.c
			
			$ ./sysenter_step		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Segmentation fault (core dumped) The program is expected to crash, and the #DB handler will issue a warning. Kernel log: WARNING: CPU: 27 PID: 7000 at arch/x86/kernel/traps.c:1009 exc_debug_kernel+0xd2/0x160 ... RIP: 0010:exc_debug_kernel+0xd2/0x160 ... Call Trace: <#DB> ? show_regs+0x68/0x80 ? __warn+0x8c/0x140 ? exc_debug_kernel+0xd2/0x160 ? report_bug+0x175/0x1a0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? handle_bug+0x44/0x90 ? exc_invalid_op+0x1c/0x70 ? asm_exc_invalid_op+0x1f/0x30 ? exc_debug_kernel+0xd2/0x160 exc_debug+0x43/0x50 asm_exc_debug+0x1e/0x40 RIP: 0010:clear_bhb_loop+0x0/0xb0 ... </#DB> <TASK> ? entry_SYSENTER_compat_after_hwframe+0x6e/0x8d </TASK> [bp: Massage commit message.] **CVE ID: CVE-2024-42240**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.100					
Use After Free	07-Aug-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/1177afeca833174ba83504688	O-LIN-LINU-080824/2105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: libceph: fix race between delayed_work() and ceph_monc_stop() The way the delayed work is handled in ceph_monc_stop() is prone to races with mon_fault() and possibly also finish_hunting(). Both of these can requeue the delayed work which wouldn't be canceled by any of the following code in case that happens after cancel_delayed_work_sync() runs -- __close_session() doesn't mess with the delayed work in order to avoid interfering with the hunting interval logic. This part was missed in commit b5d91704f53e	eec898c6214f4bf, https://git.kernel.org/stable/c/20cf67dcb7db842f941eff1af6ee5e9dc41796d7, https://git.kernel.org/stable/c/2d33654d40a05afd91ab24c9a73ab512a0670a9a	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			("libceph: behave in mon_fault() if cur_mon < 0") and use-after-free can still ensue on monc and objects that hang off of it, with monc->auth and monc->monmap being particularly susceptible to quickly being reused. To fix this: - clear monc->cur_mon and monc->hunting as part of closing the session in ceph_monc_stop() - bail from delayed_work() if monc->cur_mon is cleared, similar to how it's done in mon_fault() and finish_hunting() (based on monc->hunting) - call cancel_delayed_work_sync() after the session is closed **CVE ID: CVE-2024-42232**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: configfs: Prevent OOB read/write in usb_string_copy() Userspace provided string 's' could trivially have the length zero. Left unchecked this will firstly result in an OOB read in the form `if (str[0 - 1] == '\n')` followed closely by an OOB write in the form `str[0 - 1] = '\0'`. There is already a validating check to catch strings that are too long. Let's supply an additional check for invalid strings that are too short. **CVE ID: CVE-2024-42236**	https://git.kernel.org/stable/c/2d16f63d8030903e5031853e79d731ee5d474e70, https://git.kernel.org/stable/c/6d3c721e686ea6c59e18289b400cc95c76e927e0, https://git.kernel.org/stable/c/72b8ee0d9826e8ed00e0bdfce3e46b98419b37ce	O-LIN-LINU-080824/2106
Buffer Copy without Checking Size of Input	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/6eabd23383805725eff416c203688b7a390d4153,	O-LIN-LINU-080824/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			firmware: cs_dsp: Return error if block header overflows file Return an error from cs_dsp_power_up() if a block header is longer than the amount of data left in the file. The previous code in cs_dsp_load() and cs_dsp_load_coeff() would loop while there was enough data left in the file for a valid region. This protected against overrunning the end of the file data, but it didn't abort the file processing with an error. **CVE ID: CVE-2024-42238**	https://git.kernel.org/stable/c/90ab191b7d181057d71234e8632e06b5844ac38e, https://git.kernel.org/stable/c/959fe01e85b7241e3ec305d657febbe82da16a02	
N/A	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: USB: serial: mos7840: fix crash on resume	https://git.kernel.org/stable/c/1094ed500987e67a9d18b0f95e1812f1cc720856, https://git.kernel.org/stable/c/553e67dec846323b5575e78a7	O-LIN-LINU-080824/2108

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Since commit c49cfa917025 ("USB: serial: use generic method if no alternative is provided in usb serial layer"), USB serial core calls the generic resume implementation when the driver has not provided one. This can trigger a crash on resume with mos7840 since support for multiple read URBs was added back in 2011. Specifically, both port read URBs are now submitted on resume for open ports, but the context pointer of the second URB is left set to the core rather than mos7840 port structure. Fix this by implementing dedicated suspend and resume functions for mos7840.	76cf594c13f98c4, https://git.kernel.org/stable/c/5ae6a64f18211851c8df6b4221381c438b9a7348	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tested with Delock 87414 USB 2.0 to 4x serial adapter. [johan: analyse crash and rewrite commit message; set busy flag on resume; drop bulk-in check; drop unnecessary usb_kill_urb()] **CVE ID: CVE-2024-42244**		
Allocation of Resources Without Limits or Throttling	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: wireguard: allowedips: avoid unaligned 64-bit memory accesses On the parisc platform, the kernel issues kernel warnings because swap_endian() tries to load a 128-bit IPv6 address from an unaligned memory location: Kernel: unaligned access to 0x55f4688c in wg_allowedips_ins	https://git.kernel.org/stable/c/217978a29c6ceca76d3c640bf94bdf50c268d801, https://git.kernel.org/stable/c/2fb34bf76431e831f9863cd59adc0bd1f67b0fbf, https://git.kernel.org/stable/c/6638a203abad35fa636d59ac47bdbc4bc100fd74	O-LIN-LINU-080824/2109

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ert_v6+0x2c/0x80 [wireguard] (iir 0xf3010df) Kernel: unaligned access to 0x55f46884 in wg_allowedips_ins ert_v6+0x38/0x80 [wireguard] (iir 0xf2010dc) Avoid such unaligned memory accesses by instead using the get_unaligned_be6 4() helper macro. [Jason: replace src[8] in original patch with src+8] **CVE ID: CVE-2024-42247**		
Affected Version(s): From (including) 5.17 Up to (excluding) 6.1.100					
Excessive Iteration	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: firmware: cs_dsp: Validate payload length before processing block Move the payload length check in cs_dsp_load() and cs_dsp_coeff_load()	https://git.kern el.org/stable/c/ 259955eca9b7a cf1299b1ac077 d8cfbe12df35d 8, https://git.kern el.org/stable/c/ 3a9cd924aec12 88d675df721f2 44da4dd7e16cff , https://git.kern el.org/stable/c/ 6598afa9320b6 ab1304161695	O-LIN-LINU-080824/2110

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to be done before the block is processed. The check that the length of a block payload does not exceed the number of remaining bytes in the firwmware file buffer was being done near the end of the loop iteration. However, some code before that check used the length field without validating it. **CVE ID: CVE-2024-42237**	0ca5f8f938c0cf1	
Affected Version(s): From (including) 5.17 Up to (excluding) 6.6.41					
Allocation of Resources Without Limits or Throttling	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/shmem: disable PMD-sized page cache if needed For shmem files, it's possible that PMD-sized page cache can't be supported by xarray. For example, 512MB page cache on	https://git.kernel.org/stable/c/93893eacb372b0a4a30f7de6609b08c3ba6c4fd9, https://git.kernel.org/stable/c/9fd154ba926b34c833b7bfc4c14ee2e931b3d743, https://git.kernel.org/stable/c/cd25208ca9b0097f8e079d692fc678f36fdbc3f9	O-LIN-LINU-080824/2111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ARM64 when the base page size is 64KB can't be supported by xarray. It leads to errors as the following messages indicate when this sort of xarray entry is split. WARNING: CPU: 34 PID: 7578 at lib/xarray.c:1025 xas_split_alloc+0xf8/0x128 Modules linked in: binfmt_misc nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 \ nft_fib nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject \ nft_ct nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 \ ip_set rfkill nf_tables nfnetlink vfat fat virtio_balloon drm fuse xfs \ libcrc32c crct10dif_ce ghash_ce sha2_ce sha256_arm64 sha1_ce virtio_net \		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net_failover virtio_console virtio_blk failover dimlib virtio_mmio CPU: 34 PID: 7578 Comm: test Kdump: loaded Tainted: G W 6.10.0-rc5-gavin+ #9 Hardware name: QEMU KVM Virtual Machine, BIOS edk2-20240524-1.el9 05/24/2024 pstate: 83400005 (Nzcv daif +PAN -UAO +TCO +DIT -SSBS BTYPE=--) pc : xas_split_alloc+0xf8/0x128 lr : split_huge_page_to_list_to_order+0x1c4/0x720 sp : ffff8000882af5f0 x29: ffff8000882af5f0 x28: ffff8000882af650 x27: ffff8000882af768 x26: 0000000000000cc0 x25: 000000000000000d x24: ffff00010625b858 x23: ffff8000882af650		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x22: ffffffdfc0900000 x21: 0000000000000000 x20: 0000000000000000 x19: ffffffdfc0900000 x18: 0000000000000000 x17: 0000000000000000 x16: 0000018000000000 x15: 52f8004000000000 x14: 0000e0000000000 x13: 0000000000002000 x12: 0000000000000020 x11: 52f8000000000000 x10: 52f8e1c0ffff6000 x9 : ffffbeb9619a681c x8 : 0000000000000003 x7 : 0000000000000000 x6 : ffff00010b02ddb0 x5 : ffffbeb96395e378 x4 : 0000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0 x3 : 0000000000000cc0 x2 : 000000000000000d x1 : 000000000000000c x0 : 0000000000000000 Call trace: xas_split_alloc+0xf8/0x128 split_huge_page_to_list_to_order+0x1c4/0x720 truncate_inode_partial_folio+0xdc/0x160 shmem_undo_range+0x2bc/0x6a8 shmem_fallocate+0x134/0x430 vfs_fallocate+0x124/0x2e8 ksys_fallocate+0x4c/0xa0 __arm64_sys_fallocate+0x24/0x38 invoke_syscall.constprop.0+0x7c/0xd8		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_el0_svc+0xb4/0xd0 el0_svc+0x44/0x1d8 el0t_64_sync_handler+0x134/0x150 el0t_64_sync+0x17c/0x180 Fix it by disabling PMD-sized page cache when HPAGE_PMD_ORDER is larger than MAX_PAGECACHE_ORDER. As Matthew Wilcox pointed, the page cache in a shmem file isn't represented by a multi-index entry and doesn't have this limitation when the xarry entry is split until commit 6b24ca4a1a8d ("mm: Use multi-index entries in the page cache"). **CVE ID: CVE-2024-42241**		
Affected Version(s): From (including) 5.18 Up to (excluding) 6.6.41					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/filemap: make MAX_PAGECACHE_ ORDER acceptable to xarray Patch series "mm/filemap: Limit page cache size to that supported by xarray", v2. Currently, xarray can't support arbitrary page cache size. More details can be found from the WARN_ON() statement in xas_split_alloc(). In our test whose code is attached below, we hit the WARN_ON() on ARM64 system where the base page size is 64KB and huge page size is 512MB. The issue was reported long time ago and some discussions on it can be found here	https://git.kernel.org/stable/c/099d90642a711caae377f53309abfe27e8724a8b, https://git.kernel.org/stable/c/333c5539a31f48828456aa9997ec2808f06a699a, https://git.kernel.org/stable/c/a0c42ddd0969fdc760a85e20e267776028a7ca4e	O-LIN-LINU-080824/2112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[1]. [1] https://www.spinics.net/lists/linux-xfs/msg75404.html In order to fix the issue, we need to adjust MAX_PAGECACHE_ORDER to one supported by xarray and avoid PMD-sized page cache if needed. The code changes are suggested by David Hildenbrand. PATCH[1] adjusts MAX_PAGECACHE_ORDER to that supported by xarray PATCH[2-3] avoids PMD-sized page cache in the synchronous readahead path PATCH[4] avoids PMD-sized page cache for shmem files if needed Test program ==========		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			# cat test.c
			#define _GNU_SOURCE
			#include <stdio.h>
			#include <stdlib.h>
			#include <unistd.h>
			#include <string.h>
			#include <fcntl.h>
			#include <errno.h>
			#include <sys/syscall.h>
			#include <sys/mman.h>
			
			#define TEST_XFS_FILENAME "/tmp/data"
			#define TEST_SHMEM_FILENAME "/dev/shm/data"
			#define TEST_MEM_SIZE 0x20000000
			
			int main(int argc, char **argv)
			{
			const char *filename;
			int fd = 0;
			void *buf = (void *)-1, *p;		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			int pgsize = getpagesize();
			int ret;
			
			if (pgsize != 0x10000) {
			
			fprintf(stderr, "64KB base page size is required\n");
			
			return -EPERM;
			}
			
			system("echo force > /sys/kernel/mm/transparent_hugepage/shmem_enabled");
			system("rm -fr /tmp/data");
			system("rm -fr /dev/shm/data");
			system("echo 1 > /proc/sys/vm/drop_caches");
			
			/* Open xfs or shmem file */
			filename = TEST_XFS_FILENAME;
			if (argc > 1 &&		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			!strcmp(argv[1], "shmem"))
			
			filename = TEST_SHMEM_FILENAME;
			
			fd = open(filename, O_CREAT | O_RDWR | O_TRUNC);
			if (fd < 0) {
			
			fprintf(stderr, "Unable to open <%s>\n", filename);
			
			return -EIO;
			}
			
			/* Extend file size */
			ret = ftruncate(fd, TEST_MEM_SIZE);
			if (ret) {
			
			fprintf(stderr, "Error %d to ftruncate()\n", ret);
			goto cleanup;
			}
			
			/* Create VMA */		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			buf = mmap(NULL, TEST_MEM_SIZE, PROT_READ | PROT_WRITE, MAP_SHARED, fd, 0);
			if (buf == (void *)-1) {
			fprintf(stderr, "Unable to mmap <%s>\n", filename);
			goto cleanup;
			}
			fprintf(stdout, "mapped buffer at 0x%p\n", buf);
			ret = madvise(buf, TEST_MEM_SIZE, MADV_HUGEPAGE);
			if (ret) {
			fprintf(stderr, "Unable to madvise(MADV_HUGEPAGE)\n");
			goto cleanup;
			}
			/* Populate VMA */		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			ret = madvise(buf, TEST_MEM_SIZE, MADV_POPULATE_WRITE);
			if (ret) {
			fprintf(stderr, "Error %d to madvise(MADV_POPULATE_WRITE)\n", ret);
			goto cleanup;
			}
			/* Punch the file to enforce xarray split */
			ret = fallocate(fd, FALLOC_FL_KEEP_SIZE | FALLOC_FL_PUNCH_HOLE,
			TEST_MEM_SIZE - pgsize, pgsize);
			if (ret)
			fprintf(stderr, "Error %d to fallocate()\n", ret);
			cleanup:
			if (buf != (void *)-1)		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			munmap(buf, TEST_MEM_SIZE);
			if (fd > 0)
			close(fd);
			return 0;
			}
			
			# gcc test.c -o test
			# cat /proc/1/smaps | grep KernelPageSize | head -n 1
			KernelPageSize: 64 kB
			# ./test shmem
			:
			----------[cut here]----------
			WARNING: CPU: 17 PID: 5253 at lib/xarray.c:1025 xas_split_alloc+0xf8/0x128
			Modules linked in: nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib \
			nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject nft_ct \
			nft_chain_nat nf_nat nf_conntrack		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nf_defrag_ipv6 nf_defrag_ipv4 \ ip_set nf_tables rfkill nfnetlink vfat fat virtio_balloon \ drm fuse xfs libcrc32c crct10dif_ce ghash_ce sha2_ce sha256_arm64 \ virtio_net sha1_ce net_failover failover virtio_console virtio_blk \ dimlib virtio_mmio CPU: 17 PID: 5253 Comm: test Kdump: loaded Tainted: G W 6.10.0-rc5-gavin+ #12 Hardware name: QEMU KVM Virtual Machine, BIOS edk2-20240524-1.el9 05/24/2024 pstate: 83400005 (Nzcv daif +PAN -UAO +TC ---truncated--- **CVE ID: CVE-2024-42243**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.222					
Use After Free	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1177afeca833174ba83504688eec898c6214f4bf,	O-LIN-LINU-080824/2113

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			libceph: fix race between delayed_work() and ceph_monc_stop() The way the delayed work is handled in ceph_monc_stop() is prone to races with mon_fault() and possibly also finish_hunting(). Both of these can requeue the delayed work which wouldn't be canceled by any of the following code in case that happens after cancel_delayed_work_sync() runs -- __close_session() doesn't mess with the delayed work in order to avoid interfering with the hunting interval logic. This part was missed in commit b5d91704f53e ("libceph: behave in mon_fault() if cur_mon < 0") and use-after-free can	https://git.kernel.org/stable/c/20cf67dcb7db842f941eff1af6ee5e9dc41796d7, https://git.kernel.org/stable/c/2d33654d40a05afd91ab24c9a73ab512a0670a9a	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			still ensue on monc and objects that hang off of it, with monc->auth and monc->monmap being particularly susceptible to quickly being reused. To fix this: - clear monc->cur_mon and monc->hunting as part of closing the session in ceph_monc_stop() - bail from delayed_work() if monc->cur_mon is cleared, similar to how it's done in mon_fault() and finish_hunting() (based on monc->hunting) - call cancel_delayed_work_sync() after the session is closed **CVE ID: CVE-2024-42232**		
Out-of-bounds Write	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/2d16f63d8030903e5031853e7	O-LIN-LINU-080824/2114

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			usb: gadget: configfs: Prevent OOB read/write in usb_string_copy() Userspace provided string 's' could trivially have the length zero. Left unchecked this will firstly result in an OOB read in the form `if (str[0 - 1] == '\n') followed closely by an OOB write in the form `str[0 - 1] = '\0'`. There is already a validating check to catch strings that are too long. Let's supply an additional check for invalid strings that are too short. **CVE ID: CVE-2024-42236**	9d731ee5d474e70, https://git.kernel.org/stable/c/6d3c721e686ea6c59e18289b400cc95c76e927e0, https://git.kernel.org/stable/c/72b8ee0d9826e8ed00e0bdfce3e46b98419b37ce	
Affected Version(s): From (including) 5.6 Up to (excluding) 5.10.222					
Allocation of Resources Without Limits or Throttling	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: wireguard: allowedips: avoid	https://git.kernel.org/stable/c/217978a29c6ceca76d3c640bf94bdf50c268d801, https://git.kernel.org/stable/c/2fb34bf76431e	O-LIN-LINU-080824/2115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unaligned 64-bit memory accesses On the parisc platform, the kernel issues kernel warnings because swap_endian() tries to load a 128-bit IPv6 address from an unaligned memory location: Kernel: unaligned access to 0x55f4688c in wg_allowedips_insert_v6+0x2c/0x80 [wireguard] (iir 0xf3010df) Kernel: unaligned access to 0x55f46884 in wg_allowedips_insert_v6+0x38/0x80 [wireguard] (iir 0xf2010dc) Avoid such unaligned memory accesses by instead using the get_unaligned_be64() helper macro. [Jason: replace src[8] in original patch with src+8]	831f9863cd59adc0bd1f67b0fbf, https://git.kernel.org/stable/c/6638a203abad35fa636d59ac47bdbc4bc100fd74	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42247		
Affected Version(s): From (including) 6.1 Up to (excluding) 6.1.100					
Improper Locking	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Revert "sched/fair: Make sure to try to detach at least one movable task" This reverts commit b0defa7ae03ecf91b8bfd10ede430cff12fcbd06. b0defa7ae03ec changed the load balancing logic to ignore env.max_loop if all tasks examined to that point were pinned. The goal of the patch was to make it more likely to be able to detach a task buried in a long list of pinned tasks. However, this has the unfortunate side effect of creating an O(n) iteration in detach_tasks(), as we now must fully	https://git.kernel.org/stable/c/0fa6dcbfa2e2b97c1e6febbea561badf0931a38b, https://git.kernel.org/stable/c/1e116c18e32b035a2d1bd460800072c8bf96bc44, https://git.kernel.org/stable/c/2feab2492deb2f14f9675dd6388e9e2bf669c27a	O-LIN-LINU-080824/2116

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iterate every task on a cpu if all or most are pinned. Since this load balance code is done with rq lock held, and often in softirq context, it is very easy to trigger hard lockups. We observed such hard lockups with a user who affined O(10k) threads to a single cpu. When I discussed this with Vincent he initially suggested that we keep the limit on the number of tasks to detach, but increase the number of tasks we can search. However, after some back and forth on the mailing list, he recommended we instead revert the original patch, as it seems likely no one was actually getting hit by the original issue.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42245		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.41					
Use After Free	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: libceph: fix race between delayed_work() and ceph_monc_stop() The way the delayed work is handled in ceph_monc_stop() is prone to races with mon_fault() and possibly also finish_hunting(). Both of these can requeue the delayed work which wouldn't be canceled by any of the following code in case that happens after cancel_delayed_work_sync() runs -- __close_session() doesn't mess with the delayed work in order to avoid interfering with the hunting	https://git.kernel.org/stable/c/1177afeca833174ba83504688eec898c6214f4bf, https://git.kernel.org/stable/c/20cf67dcb7db842f941eff1af6ee5e9dc41796d7, https://git.kernel.org/stable/c/2d33654d40a05afd91ab24c9a73ab512a0670a9a	O-LIN-LINU-080824/2117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interval logic. This part was missed in commit b5d91704f53e ("libceph: behave in mon_fault() if cur_mon < 0") and use-after-free can still ensue on monc and objects that hang off of it, with monc->auth and monc->monmap being particularly susceptible to quickly being reused. To fix this: - clear monc->cur_mon and monc->hunting as part of closing the session in ceph_monc_stop() - bail from delayed_work() if monc->cur_mon is cleared, similar to how it's done in mon_fault() and finish_hunting() (based on monc->hunting) - call cancel_delayed_wo		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rk_sync() after the session is closed **CVE ID: CVE-2024-42232**		
Out-of-bounds Write	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: configfs: Prevent OOB read/write in usb_string_copy() Userspace provided string 's' could trivially have the length zero. Left unchecked this will firstly result in an OOB read in the form `if (str[0 - 1] == '\n') followed closely by an OOB write in the form `str[0 - 1] = '\0'`. There is already a validating check to catch strings that are too long. Let's supply an additional check for invalid strings that are too short. **CVE ID: CVE-2024-42236**	https://git.kernel.org/stable/c/2d16f63d8030903e5031853e79d731ee5d474e70, https://git.kernel.org/stable/c/6d3c721e686ea6c59e18289b400cc95c76e927e0, https://git.kernel.org/stable/c/72b8ee0d9826e8ed00e0bdfce3e46b98419b37ce	O-LIN-LINU-080824/2118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Excessive Iteration	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: firmware: cs_dsp: Validate payload length before processing block Move the payload length check in cs_dsp_load() and cs_dsp_coeff_load() to be done before the block is processed. The check that the length of a block payload does not exceed the number of remaining bytes in the firwmware file buffer was being done near the end of the loop iteration. However, some code before that check used the length field without validating it. **CVE ID: CVE-2024-42237**	https://git.kernel.org/stable/c/259955eca9b7acf1299b1ac077d8cfbe12df35d8, https://git.kernel.org/stable/c/3a9cd924aec1288d675df721f244da4dd7e16cff, https://git.kernel.org/stable/c/6598afa9320b6ab13041616950ca5f8f938c0cf1	O-LIN-LINU-080824/2119
Buffer Copy without Checking Size of Input	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/6eabd23383805725eff416c203688b7a390d4153,	O-LIN-LINU-080824/2120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			firmware: cs_dsp: Return error if block header overflows file Return an error from cs_dsp_power_up() if a block header is longer than the amount of data left in the file. The previous code in cs_dsp_load() and cs_dsp_load_coeff() would loop while there was enough data left in the file for a valid region. This protected against overrunning the end of the file data, but it didn't abort the file processing with an error. **CVE ID: CVE-2024-42238**	https://git.kernel.org/stable/c/90ab191b7d181057d71234e8632e06b5844ac38e, https://git.kernel.org/stable/c/959fe01e85b7241e3ec305d657febbe82da16a02	
Loop with Unreachable Exit Condition ('Infinite Loop')	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: x86/bhi: Avoid warning in #DB handler due to BHI mitigation	https://git.kernel.org/stable/c/08518d48e5b744620524f0acd7c26c19bda7f513, https://git.kernel.org/stable/c/a765679defe1dc1b8fa01928a6	O-LIN-LINU-080824/2121

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When BHI mitigation is enabled, if SYSENTER is invoked with the TF flag set then entry_SYSENTER_compat() uses CLEAR_BRANCH_HISTORY and calls the clear_bhb_loop() before the TF flag is cleared. This causes the #DB handler (exc_debug_kernel()) to issue a warning because single-step is used outside the entry_SYSENTER_compat() function. To address this issue, entry_SYSENTER_compat() should use CLEAR_BRANCH_HISTORY after making sure the TF flag is cleared. The problem can be reproduced with the following sequence:	ad6361e72a1364, https://git.kernel.org/stable/c/ac8b270b61d48fcc61f052097777e3b5e11591e0	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			$ cat sysenter_step.c
			int main()
			{ asm("pushf; pop %ax; bts $8,%ax; push %ax; popf; sysenter"); }
			
			$ gcc -o sysenter_step sysenter_step.c
			
			$ ./sysenter_step
			Segmentation fault (core dumped)
			
			The program is expected to crash, and the #DB handler will issue a warning.
			
			Kernel log:
			
			WARNING: CPU: 27 PID: 7000 at arch/x86/kernel/traps.c:1009 exc_debug_kernel+0xd2/0x160
			...
			RIP: 0010:exc_debug_kernel+0xd2/0x160
			...
			Call Trace:
			<#DB>		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? show_regs+0x68/0x80 ? __warn+0x8c/0x140 ? exc_debug_kernel+0xd2/0x160 ? report_bug+0x175/0x1a0 ? handle_bug+0x44/0x90 ? exc_invalid_op+0x1c/0x70 ? asm_exc_invalid_op+0x1f/0x30 ? exc_debug_kernel+0xd2/0x160 exc_debug+0x43/0x50 asm_exc_debug+0x1e/0x40 RIP: 0010:clear_bhb_loop+0x0/0xb0 ... </#DB> <TASK> ? entry_SYSENTER_c		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ompat_after_hwframe+0x6e/0x8d </TASK> [bp: Massage commit message.] **CVE ID: CVE-2024-42240**		
N/A	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: USB: serial: mos7840: fix crash on resume Since commit c49cfa917025 ("USB: serial: use generic method if no alternative is provided in usb serial layer"), USB serial core calls the generic resume implementation when the driver has not provided one. This can trigger a crash on resume with mos7840 since support for multiple read URBs was added back in 2011. Specifically, both port read	https://git.kernel.org/stable/c/1094ed500987e67a9d18b0f95e1812f1cc720856, https://git.kernel.org/stable/c/553e67dec846323b5575e78a776cf594c13f98c4, https://git.kernel.org/stable/c/5ae6a64f18211851c8df6b4221381c438b9a7348	O-LIN-LINU-080824/2122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			URBs are now submitted on resume for open ports, but the context pointer of the second URB is left set to the core rather than mos7840 port structure. Fix this by implementing dedicated suspend and resume functions for mos7840. Tested with Delock 87414 USB 2.0 to 4x serial adapter. [johan: analyse crash and rewrite commit message; set busy flag on resume; drop bulk-in check; drop unnecessary usb_kill_urb()] **CVE ID: CVE-2024-42244**		
Improper Locking	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Revert "sched/fair: Make sure to try to	https://git.kernel.org/stable/c/0fa6dcbfa2e2b97c1e6febbea561badf0931a38b, https://git.kernel.org/stable/c/1e116c18e32b0	O-LIN-LINU-080824/2123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			detach at least one movable task" This reverts commit b0defa7ae03ecf91b8bfd10ede430cff12fcbd06. b0defa7ae03ec changed the load balancing logic to ignore env.max_loop if all tasks examined to that point were pinned. The goal of the patch was to make it more likely to be able to detach a task buried in a long list of pinned tasks. However, this has the unfortunate side effect of creating an O(n) iteration in detach_tasks(), as we now must fully iterate every task on a cpu if all or most are pinned. Since this load balance code is done with rq lock held, and often in softirq context, it is very easy to trigger hard	35a2d1bd460800072c8bf96bc44, https://git.kernel.org/stable/c/2feab2492deb2f14f9675dd6388e9e2bf669c27a	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lockups. We observed such hard lockups with a user who affined O(10k) threads to a single cpu. When I discussed this with Vincent he initially suggested that we keep the limit on the number of tasks to detach, but increase the number of tasks we can search. However, after some back and forth on the mailing list, he recommended we instead revert the original patch, as it seems likely no one was actually getting hit by the original issue. **CVE ID: CVE-2024-42245**		
Loop with Unreachable Exit Condition ('Infinite Loop')	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net, sunrpc: Remap EPERM in case of connection failure	https://git.kernel.org/stable/c/626dfed5fa3bfb41e0dffd796032b555b69f9cde, https://git.kernel.org/stable/c/d6c686c01c5f12ff8f7264e0ddf	O-LIN-LINU-080824/2124

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in xs_tcp_setup_socket When using a BPF program on kernel_connect(), the call can return -EPERM. This causes xs_tcp_setup_socket() to loop forever, filling up the syslog and causing the kernel to potentially freeze up. Neil suggested: This will propagate -EPERM up into other layers which might not be ready to handle it. It might be safer to map EPERM to an error we would be more likely to expect from the network system - such as ECONNREFUSED or ENETDOWN. ECONNREFUSED as error seems reasonable. For	71df6cb0d4414, https://git.kernel.org/stable/c/f2431e7db0fe0daccb2f06bb0d23740affcd2fa6	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			programs setting a different error can be out of reach (see handling in 4fbac77d2d09) in particular on kernels which do not have f10d05966196 ("bpf: Make BPF_PROG_RUN_ARRAY return -err instead of allow boolean"), thus given that it is better to simply remap for consistent behavior. UDP does handle EPERM in xs_udp_send_request(). **CVE ID: CVE-2024-42246**		
Allocation of Resources Without Limits or Throttling	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: wireguard: allowedips: avoid unaligned 64-bit memory accesses On the parisc platform, the kernel issues kernel warnings because swap_endian() tries to load a 128-	https://git.kernel.org/stable/c/217978a29c6ceca76d3c640bf94bdf50c268d801, https://git.kernel.org/stable/c/2fb34bf76431e831f9863cd59adc0bd1f67b0fbf, https://git.kernel.org/stable/c/6638a203abad35fa636d59ac47bdbc4bc100fd74	O-LIN-LINU-080824/2125

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bit IPv6 address from an unaligned memory location: Kernel: unaligned access to 0x55f4688c in wg_allowedips_insert_v6+0x2c/0x80 [wireguard] (iir 0xf3010df) Kernel: unaligned access to 0x55f46884 in wg_allowedips_insert_v6+0x38/0x80 [wireguard] (iir 0xf2010dc) Avoid such unaligned memory accesses by instead using the get_unaligned_be64() helper macro. [Jason: replace src[8] in original patch with src+8] **CVE ID: CVE-2024-42247**		
Affected Version(s): From (including) 6.5 Up to (excluding) 6.6.41					
NULL Pointer Dereference	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0e0e15ab2d3a094a38525d23c03d78ec7d14a40e, https://git.kernel.org/stable/c/	O-LIN-LINU-080824/2126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tty: serial: ma35d1: Add a NULL check for of_node The pdev->dev.of_node can be NULL if the "serial" node is absent. Add a NULL check to return an error in such cases. **CVE ID: CVE-2024-42248**	23efa74cfe6eb923abb5b9bc51b2a04879013c67, https://git.kernel.org/stable/c/acd09ac253b5de8fd79fc61a482ee19154914c7a	
Affected Version(s): From (including) 6.6 Up to (excluding) 6.6.41					
NULL Pointer Dereference	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: s390/mm: Add NULL pointer check to crst_table_free() base_crst_free() crst_table_free() used to work with NULL pointers before the conversion to ptdescs. Since crst_table_free() can be called with a NULL pointer (error handling in crst_table_upgrade() add an explicit check.	https://git.kernel.org/stable/c/794fa52b94637d6b2e8c9474fbe3983af5c9f046, https://git.kernel.org/stable/c/b5efb63acf7bddaf20eacfcac654c25c446eabe8, https://git.kernel.org/stable/c/f80bd8bb6f380bc265834c46058d38b34174813e	O-LIN-LINU-080824/2127

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Also add the same check to base_crst_free() for consistency reasons. In real life this should not happen, since order two GFP_KERNEL allocations will not fail, unless FAIL_PAGE_ALLOC is enabled and used. **CVE ID: CVE-2024-42235**		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.9.10					
Use After Free	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: libceph: fix race between delayed_work() and ceph_monc_stop() The way the delayed work is handled in ceph_monc_stop() is prone to races with mon_fault() and possibly also finish_hunting(). Both of	https://git.kernel.org/stable/c/1177afeca833174ba83504688eec898c6214f4bf, https://git.kernel.org/stable/c/20cf67dcb7db842f941eff1af6ee5e9dc41796d7, https://git.kernel.org/stable/c/2d33654d40a05afd91ab24c9a73ab512a0670a9a	O-LIN-LINU-080824/2128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these can requeue the delayed work which wouldn't be canceled by any of the following code in case that happens after cancel_delayed_work_sync() runs --__close_session() doesn't mess with the delayed work in order to avoid interfering with the hunting interval logic. This part was missed in commit b5d91704f53e ("libceph: behave in mon_fault() if cur_mon < 0") and use-after-free can still ensue on monc and objects that hang off of it, with monc->auth and monc->monmap being particularly susceptible to quickly being reused. To fix this: - clear monc->cur_mon and monc->hunting as		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			part of closing the session in ceph_monc_stop() - bail from delayed_work() if monc->cur_mon is cleared, similar to how it's done in mon_fault() and finish_hunting() (based on monc->hunting) - call cancel_delayed_work_sync() after the session is closed **CVE ID: CVE-2024-42232**		
Double Free	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm: fix crashes from deferred split racing folio migration Even on 6.10-rc6, I've been seeing elusive "Bad page state"s (often on flags when freeing, yet the flags shown are not bad: PG_locked had been set and cleared??), and	https://git.kernel.org/stable/c/be9581ea8c058d81154251cb0695987098996cad, https://git.kernel.org/stable/c/fc7facce686b64201dbf0b9614cc1d0bfad70010	O-LIN-LINU-080824/2129

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VM_BUG_ON_PAGE (page_ref_count(page) == 0)s from deferred_split_scan ()'s folio_put(), and a variety of other BUG and WARN symptoms implying double free by deferred split and large folio migration. 6.7 commit 9bcef5973e31 ("mm: memcg: fix split queue list crash when large folio migration") was right to fix the memcg-dependent locking broken in 85ce2c517ade ("memcontrol: only transfer the memcg data for migration"), but missed a subtlety of deferred_split_scan (): it moves folios to its own local list to work on them without split_queue_lock, during which time folio->_deferred_list is not empty, but even the "right" lock does nothing		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to secure the folio and the list it is on. Fortunately, deferred_split_scan() is careful to use folio_try_get(): so folio_migrate_mapping() can avoid the race by folio_undo_large_rmappable() while the old folio's reference count is temporarily frozen to 0 - adding such a freeze in the !mapping case too (originally, folio lock and unmapping and no swap cache left an anon folio unreachable, so no freezing was needed there: but the deferred split queue offers a way to reach it). **CVE ID: CVE-2024-42234**		
NULL Pointer Dereference	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: s390/mm: Add NULL pointer check to crst_table_free() base_crst_free()	https://git.kernel.org/stable/c/794fa52b94637d6b2e8c9474fbe3983af5c9f046, https://git.kernel.org/stable/c/b5efb63acf7bddaf20eacfcac654	O-LIN-LINU-080824/2130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crst_table_free() used to work with NULL pointers before the conversion to ptdescs. Since crst_table_free() can be called with a NULL pointer (error handling in crst_table_upgrade() add an explicit check. Also add the same check to base_crst_free() for consistency reasons. In real life this should not happen, since order two GFP_KERNEL allocations will not fail, unless FAIL_PAGE_ALLOC is enabled and used. **CVE ID: CVE-2024-42235**	c25c446eabe8, https://git.kernel.org/stable/c/f80bd8bb6f380bc265834c46058d38b34174813e	
Out-of-bounds Write	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: configfs: Prevent	https://git.kernel.org/stable/c/2d16f63d8030903e5031853e79d731ee5d474e70, https://git.kernel.org/stable/c/6d3c721e686ea	O-LIN-LINU-080824/2131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OOB read/write in usb_string_copy() Userspace provided string 's' could trivially have the length zero. Left unchecked this will firstly result in an OOB read in the form `if (str[0 - 1] == '\n') followed closely by an OOB write in the form `str[0 - 1] = '\0'`. There is already a validating check to catch strings that are too long. Let's supply an additional check for invalid strings that are too short. **CVE ID: CVE-2024-42236**	6c59e18289b400cc95c76e927e0, https://git.kernel.org/stable/c/72b8ee0d9826e8ed00e0bdfce3e46b98419b37ce	
Excessive Iteration	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: firmware: cs_dsp: Validate payload length before processing block Move the payload length check in	https://git.kernel.org/stable/c/259955eca9b7acf1299b1ac077d8cfbe12df35d8, https://git.kernel.org/stable/c/3a9cd924aec1288d675df721f244da4dd7e16cff, https://git.kernel.org/stable/c/	O-LIN-LINU-080824/2132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cs_dsp_load() and cs_dsp_coeff_load() to be done before the block is processed. The check that the length of a block payload does not exceed the number of remaining bytes in the firwmware file buffer was being done near the end of the loop iteration. However, some code before that check used the length field without validating it. **CVE ID: CVE-2024-42237**	6598afa9320b6ab13041616950ca5f8f938c0cf1	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: firmware: cs_dsp: Return error if block header overflows file Return an error from cs_dsp_power_up() if a block header is longer than the amount of data left in the file.	https://git.kernel.org/stable/c/6eabd23383805725eff416c203688b7a390d4153, https://git.kernel.org/stable/c/90ab191b7d181057d71234e8632e06b5844ac38e, https://git.kernel.org/stable/c/959fe01e85b7241e3ec305d657febbe82da16a02	O-LIN-LINU-080824/2133

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The previous code in cs_dsp_load() and cs_dsp_load_coeff() would loop while there was enough data left in the file for a valid region. This protected against overrunning the end of the file data, but it didn't abort the file processing with an error. **CVE ID: CVE-2024-42238**		

Improper Locking	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:
			bpf: Fail bpf_timer_cancel when callback is being cancelled
			Given a schedule:
			timer1 cb
			timer2 cb
			bpf_timer_cancel(timer2);
			bpf_timer_cancel(timer1);
				https://git.kernel.org/stable/c/3e4e8178a8666c56813bd167b848fca0f4c9af0a, https://git.kernel.org/stable/c/9369830518688ecd5b08ffc08ab3302ce2b5d0f7, https://git.kernel.org/stable/c/d4523831f07a267a943f0dde844bf8ead7495f13	O-LIN-LINU-080824/2134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Both bpf_timer_cancel calls would wait for the other callback to finish executing, introducing a lockup. Add an atomic_t count named 'cancelling' in bpf_hrtimer. This keeps track of all in-flight cancellation requests for a given BPF timer. Whenever cancelling a BPF timer, we must check if we have outstanding cancellation requests, and if so, we must fail the operation with an error (-EDEADLK) since cancellation is synchronous and waits for the callback to finish executing. This implies that we can enter a deadlock situation involving two or more timer callbacks executing in parallel		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and attempting to cancel one another. Note that we avoid incrementing the cancelling counter for the target timer (the one being cancelled) if bpf_timer_cancel is not invoked from a callback, to avoid spurious errors. The whole point of detecting cur->cancelling and returning -EDEADLK is to not enter a busy wait loop (which may or may not lead to a lockup). This does not apply in case the caller is in a non-callback context, the other side can continue to cancel as it sees fit without running into errors. Background on prior attempts: Earlier versions of this patch used a bool 'cancelling' bit and used the		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			following pattern under timer->lock to publish cancellation status.
			
			lock(t->lock);
			t->cancelling = true;
			mb();
			if (cur->cancelling)
			return -EDEADLK;
			unlock(t->lock);
			hrtimer_cancel(t->timer);
			t->cancelling = false;
			
			The store outside the critical section could overwrite a parallel
			requests t->cancelling assignment to true, to ensure the parallely
			executing callback observes its cancellation status.
			
			It would be necessary to clear this cancelling bit once hrtimer_cancel
			is done, but lack of serialization		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			introduced races. Another option was explored where bpf_timer_start would clear the bit when (re)starting the timer under timer->lock. This would ensure serialized access to the cancelling bit, but may allow it to be cleared before in-flight hrtimer_cancel has finished executing, such that lockups can occur again. Thus, we choose an atomic counter to keep track of all outstanding cancellation requests and use it to prevent lockups in case callbacks attempt to cancel each other while executing in parallel. **CVE ID: CVE-2024-42239**		
Loop with Unreachable Exit Condition	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/08518d48e5b744620524f0acd7c26c19bda7f5	O-LIN-LINU-080824/2135

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			x86/bhi: Avoid warning in #DB handler due to BHI mitigation When BHI mitigation is enabled, if SYSENTER is invoked with the TF flag set then entry_SYSENTER_compat() uses CLEAR_BRANCH_HISTORY and calls the clear_bhb_loop() before the TF flag is cleared. This causes the #DB handler (exc_debug_kernel()) to issue a warning because single-step is used outside the entry_SYSENTER_compat() function. To address this issue, entry_SYSENTER_compat() should use CLEAR_BRANCH_HISTORY after making sure the TF flag is cleared.	13, https://git.kernel.org/stable/c/a765679defe1dc1b8fa01928a6ad6361e72a1364, https://git.kernel.org/stable/c/ac8b270b61d48fcc61f052097777e3b5e11591e0	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			The problem can be reproduced with the following sequence:
			
			$ cat sysenter_step.c
			int main()
			{ asm("pushf; pop %ax; bts $8,%ax; push %ax; popf; sysenter"); }
			
			$ gcc -o sysenter_step sysenter_step.c
			
			$ ./sysenter_step
			Segmentation fault (core dumped)
			
			The program is expected to crash, and the #DB handler will issue a warning.
			
			Kernel log:
			
			WARNING: CPU: 27 PID: 7000 at arch/x86/kernel/traps.c:1009 exc_debug_kernel+0xd2/0x160
			...		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RIP: 0010:exc_debug_kernel+0xd2/0x160 ... Call Trace: <#DB> ? show_regs+0x68/0x80 ? __warn+0x8c/0x140 ? exc_debug_kernel+0xd2/0x160 ? report_bug+0x175/0x1a0 ? handle_bug+0x44/0x90 ? exc_invalid_op+0x1c/0x70 ? asm_exc_invalid_op+0x1f/0x30 ? exc_debug_kernel+0xd2/0x160 exc_debug+0x43/0x50 asm_exc_debug+0x1e/0x40 RIP: 0010:clear_bhb_loop+0x0/0xb0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			... </#DB> <TASK> ? entry_SYSENTER_compat_after_hwframe+0x6e/0x8d </TASK> [bp: Massage commit message.] **CVE ID: CVE-2024-42240**		
Allocation of Resources Without Limits or Throttling	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/shmem: disable PMD-sized page cache if needed For shmem files, it's possible that PMD-sized page cache can't be supported by xarray. For example, 512MB page cache on ARM64 when the base page size is 64KB can't be supported by xarray. It leads to errors as the following messages indicate when this	https://git.kernel.org/stable/c/93893eacb372b0a4a30f7de6609b08c3ba6c4fd9, https://git.kernel.org/stable/c/9fd154ba926b34c833b7bfc4c14ee2e931b3d743, https://git.kernel.org/stable/c/cd25208ca9b0097f8e079d692fc678f36fdbc3f9	O-LIN-LINU-080824/2136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sort of xarray entry is split. WARNING: CPU: 34 PID: 7578 at lib/xarray.c:1025 xas_split_alloc+0xf8/0x128 Modules linked in: binfmt_misc nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 \ nft_fib nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject \ nft_ct nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 \ ip_set rfkill nf_tables nfnetlink vfat fat virtio_balloon drm fuse xfs \ libcrc32c crct10dif_ce ghash_ce sha2_ce sha256_arm64 sha1_ce virtio_net \ net_failover virtio_console virtio_blk failover dimlib virtio_mmio CPU: 34 PID: 7578 Comm: test Kdump: loaded Tainted: G W 6.10.0-rc5-gavin+ #9		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hardware name: QEMU KVM Virtual Machine, BIOS edk2-20240524-1.el9 05/24/2024 pstate: 83400005 (Nzcv daif +PAN -UAO +TCO +DIT -SSBS BTYPE=--) pc : xas_split_alloc+0xf8/0x128 lr : split_huge_page_to_list_to_order+0x1c4/0x720 sp : ffff8000882af5f0 x29: ffff8000882af5f0 x28: ffff8000882af650 x27: ffff8000882af768 x26: 0000000000000cc0 x25: 000000000000000d x24: ffff00010625b858 x23: ffff8000882af650 x22: fffffdfc0900000 x21: 0000000000000000 x20: 0000000000000000 x19: fffffdfc0900000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x18: 0000000000000000 x17: 0000000000000000 x16: 0000018000000000 x15: 52f8004000000000 x14: 0000e0000000000 x13: 0000000000002000 x12: 0000000000000020 x11: 52f8000000000000 x10: 52f8e1c0ffff6000 x9 : ffffbeb9619a681c x8 : 0000000000000003 x7 : 0000000000000000 x6 : ffff00010b02ddb0 x5 : ffffbeb96395e378 x4 : 0000000000000000 x3 : 0000000000000cc0 x2 : 000000000000000d x1 : 000000000000000c x0 :		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 Call trace: xas_split_alloc+0xf8/0x128 split_huge_page_to_list_to_order+0x1c4/0x720 truncate_inode_partial_folio+0xdc/0x160 shmem_undo_range+0x2bc/0x6a8 shmem_fallocate+0x134/0x430 vfs_fallocate+0x124/0x2e8 ksys_fallocate+0x4c/0xa0 __arm64_sys_fallocate+0x24/0x38 invoke_syscall.constprop.0+0x7c/0xd8 do_el0_svc+0xb4/0xd0 el0_svc+0x44/0x1d8		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			el0t_64_sync_handler+0x134/0x150 el0t_64_sync+0x17c/0x180 Fix it by disabling PMD-sized page cache when HPAGE_PMD_ORDER is larger than MAX_PAGECACHE_ORDER. As Matthew Wilcox pointed, the page cache in a shmem file isn't represented by a multi-index entry and doesn't have this limitation when the xarry entry is split until commit 6b24ca4a1a8d ("mm: Use multi-index entries in the page cache"). **CVE ID: CVE-2024-42241**		
N/A	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/filemap: make MAX_PAGECACHE_	https://git.kernel.org/stable/c/099d90642a711caae377f53309abfe27e8724a8b, https://git.kernel.org/stable/c/	O-LIN-LINU-080824/2137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ORDER acceptable to xarray Patch series "mm/filemap: Limit page cache size to that supported by xarray", v2. Currently, xarray can't support arbitrary page cache size. More details can be found from the WARN_ON() statement in xas_split_alloc(). In our test whose code is attached below, we hit the WARN_ON() on ARM64 system where the base page size is 64KB and huge page size is 512MB. The issue was reported long time ago and some discussions on it can be found here [1]. [1] https://www.spinics.net/lists/linux-xfs/msg75404.html	333c5539a31f48828456aa9997ec2808f06a699a, https://git.kernel.org/stable/c/a0c42ddd0969fdc760a85e20e267776028a7ca4e	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In order to fix the issue, we need to adjust MAX_PAGECACHE_ ORDER to one supported by xarray and avoid PMD-sized page cache if needed. The code changes are suggested by David Hildenbrand. PATCH[1] adjusts MAX_PAGECACHE_ ORDER to that supported by xarray PATCH[2-3] avoids PMD-sized page cache in the synchronous readahead path PATCH[4] avoids PMD-sized page cache for shmem files if needed Test program ========== # cat test.c #define _GNU_SOURCE #include <stdio.h> #include <stdlib.h> #include <unistd.h>		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			#include <string.h>
			#include <fcntl.h>
			#include <errno.h>
			#include <sys/syscall.h>
			#include <sys/mman.h>
			
			#define TEST_XFS_FILENAME "/tmp/data"
			#define TEST_SHMEM_FILENAME "/dev/shm/data"
			#define TEST_MEM_SIZE 0x20000000
			
			int main(int argc, char **argv)
			{
			const char *filename;
			int fd = 0;
			void *buf = (void *)-1, *p;
			int pgsize = getpagesize();
			int ret;
			
			if (pgsize != 0x10000) {
			
			fprintf(stder		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			r, "64KB base page size is required\n");
			
			return -EPERM;
			}
			
			system("echo force > /sys/kernel/mm/transparent_hugepage/shmem_enabled");
			system("rm -fr /tmp/data");
			system("rm -fr /dev/shm/data");
			system("echo 1 > /proc/sys/vm/drop_caches");
			
			/* Open xfs or shmem file */
			filename = TEST_XFS_FILENAME;
			if (argc > 1 && !strcmp(argv[1], "shmem"))
			
			filename = TEST_SHMEM_FILENAME;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			fd = open(filename, O_CREAT | O_RDWR | O_TRUNC);
			if (fd < 0) {
			fprintf(stderr, "Unable to open <%s>\n", filename);
			return -EIO;
			}
			/* Extend file size */
			ret = ftruncate(fd, TEST_MEM_SIZE);
			if (ret) {
			fprintf(stderr, "Error %d to ftruncate()\n", ret);
			goto cleanup;
			}
			/* Create VMA */
			buf = mmap(NULL, TEST_MEM_SIZE,
			PROT_READ | PROT_WRITE, MAP_SHARED, fd, 0);		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			if (buf == (void *)-1) {
			
			fprintf(stderr, "Unable to mmap <%s>\n", filename);
			goto cleanup;
			}
			
			fprintf(stdout, "mapped buffer at 0x%p\n", buf);
			ret = madvise(buf, TEST_MEM_SIZE, MADV_HUGEPAGE);
			if (ret) {
			
			fprintf(stderr, "Unable to madvise(MADV_HUGEPAGE)\n");
			goto cleanup;
			}
			
			/* Populate VMA */
			ret = madvise(buf, TEST_MEM_SIZE, MADV_POPULATE_WRITE);
			if (ret) {
			
			fprintf(stder		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			r, "Error %d to madvise(MADV_POPULATE_WRITE)\n", ret);
			goto cleanup;
			}
			
			/* Punch the file to enforce xarray split */
			ret = fallocate(fd, FALLOC_FL_KEEP_SIZE | FALLOC_FL_PUNCH_HOLE,
			
			TEST_MEM_SIZE - pgsize, pgsize);
			if (ret)
			
			fprintf(stder r, "Error %d to fallocate()\n", ret);
			
			cleanup:
			if (buf != (void *)-1)
			
			munmap(bu f, TEST_MEM_SIZE);
			if (fd > 0)
			
			close(fd);		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			return 0; } # gcc test.c -o test # cat /proc/1/smaps | grep KernelPageSize | head -n 1 KernelPageSize: 64 kB # ./test shmem : ----------[cut here]---------- WARNING: CPU: 17 PID: 5253 at lib/xarray.c:1025 xas_split_alloc+0xf8/0x128 Modules linked in: nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib \ nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject nft_ct \ nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 \ ip_set nf_tables rfkill nfnetlink vfat fat virtio_balloon \ drm fuse xfs libcrc32c		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crct10dif_ce ghash_ce sha2_ce sha256_arm64 \ virtio_net sha1_ce net_failover failover virtio_console virtio_blk \ dimlib virtio_mmio CPU: 17 PID: 5253 Comm: test Kdump: loaded Tainted: G W 6.10.0-rc5-gavin+ #12 Hardware name: QEMU KVM Virtual Machine, BIOS edk2-20240524-1.el9 05/24/2024 pstate: 83400005 (Nzcv daif +PAN -UAO +TC ---truncated--- **CVE ID: CVE-2024-42243**		
N/A	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: USB: serial: mos7840: fix crash on resume Since commit c49cfa917025 ("USB: serial: use generic method if no	https://git.kernel.org/stable/c/1094ed500987e67a9d18b0f95e1812f1cc720856, https://git.kernel.org/stable/c/553e67dec846323b5575e78a776cf594c13f98c4, https://git.kernel.org/stable/c/5ae6a64f18211851c8df6b4221	O-LIN-LINU-080824/2138

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alternative is provided in usb serial layer"), USB serial core calls the generic resume implementation when the driver has not provided one. This can trigger a crash on resume with mos7840 since support for multiple read URBs was added back in 2011. Specifically, both port read URBs are now submitted on resume for open ports, but the context pointer of the second URB is left set to the core rather than mos7840 port structure. Fix this by implementing dedicated suspend and resume functions for mos7840. Tested with Delock 87414 USB 2.0 to 4x serial adapter.	381c438b9a7348	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[johan: analyse crash and rewrite commit message; set busy flag on resume; drop bulk-in check; drop unnecessary usb_kill_urb()] **CVE ID: CVE-2024-42244**		
Improper Locking	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Revert "sched/fair: Make sure to try to detach at least one movable task" This reverts commit b0defa7ae03ecf91b8bfd10ede430cff12fcbd06. b0defa7ae03ec changed the load balancing logic to ignore env.max_loop if all tasks examined to that point were pinned. The goal of the patch was to make it more likely to be able to detach a task buried in a long list	https://git.kernel.org/stable/c/0fa6dcbfa2e2b97c1e6febbea561badf0931a38b, https://git.kernel.org/stable/c/1e116c18e32b035a2d1bd460800072c8bf96bc44, https://git.kernel.org/stable/c/2feab2492deb2f14f9675dd6388e9e2bf669c27a	O-LIN-LINU-080824/2139

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of pinned tasks. However, this has the unfortunate side effect of creating an O(n) iteration in detach_tasks(), as we now must fully iterate every task on a cpu if all or most are pinned. Since this load balance code is done with rq lock held, and often in softirq context, it is very easy to trigger hard lockups. We observed such hard lockups with a user who affined O(10k) threads to a single cpu. When I discussed this with Vincent he initially suggested that we keep the limit on the number of tasks to detach, but increase the number of tasks we can search. However, after some back and forth on the mailing list, he recommended we		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instead revert the original patch, as it seems likely no one was actually getting hit by the original issue. **CVE ID: CVE-2024-42245**		
Loop with Unreachable Exit Condition ('Infinite Loop')	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net, sunrpc: Remap EPERM in case of connection failure in xs_tcp_setup_socket When using a BPF program on kernel_connect(), the call can return -EPERM. This causes xs_tcp_setup_socket() to loop forever, filling up the syslog and causing the kernel to potentially freeze up. Neil suggested: This will propagate -EPERM up into other layers	https://git.kernel.org/stable/c/626dfed5fa3bfb41e0dffd796032b555b69f9cde, https://git.kernel.org/stable/c/d6c686c01c5f12ff8f7264e0ddf71df6cb0d4414, https://git.kernel.org/stable/c/f2431e7db0fe0daccb2f06bb0d23740affcd2fa6	O-LIN-LINU-080824/2140

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which might not be ready to handle it. It might be safer to map EPERM to an error we would be more likely to expect from the network system - such as ECONNREFUSED or ENETDOWN. ECONNREFUSED as error seems reasonable. For programs setting a different error can be out of reach (see handling in 4fbac77d2d09) in particular on kernels which do not have f10d05966196 ("bpf: Make BPF_PROG_RUN_ARRAY return -err instead of allow boolean"), thus given that it is better to simply remap for consistent behavior. UDP does handle EPERM in xs_udp_send_request(). **CVE ID: CVE-2024-42246**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: wireguard: allowedips: avoid unaligned 64-bit memory accesses On the parisc platform, the kernel issues kernel warnings because swap_endian() tries to load a 128-bit IPv6 address from an unaligned memory location: Kernel: unaligned access to 0x55f4688c in wg_allowedips_insert_v6+0x2c/0x80 [wireguard] (iir 0xf3010df) Kernel: unaligned access to 0x55f46884 in wg_allowedips_insert_v6+0x38/0x80 [wireguard] (iir 0xf2010dc) Avoid such unaligned memory accesses by instead using the	https://git.kernel.org/stable/c/217978a29c6ceca76d3c640bf94bdf50c268d801, https://git.kernel.org/stable/c/2fb34bf76431e831f9863cd59adc0bd1f67b0fbf, https://git.kernel.org/stable/c/6638a203abad35fa636d59ac47bdbc4bc100fd74	O-LIN-LINU-080824/2141

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			get_unaligned_be64() helper macro. [Jason: replace src[8] in original patch with src+8] **CVE ID: CVE-2024-42247**		
NULL Pointer Dereference	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: tty: serial: ma35d1: Add a NULL check for of_node The pdev->dev.of_node can be NULL if the "serial" node is absent. Add a NULL check to return an error in such cases. **CVE ID: CVE-2024-42248**	https://git.kernel.org/stable/c/0e0e15ab2d3a094a38525d23c03d78ec7d14a40e, https://git.kernel.org/stable/c/23efa74cfe6eb923abb5b9bc51b2a04879013c67, https://git.kernel.org/stable/c/acd09ac253b5de8fd79fc61a482ee19154914c7a	O-LIN-LINU-080824/2142
Affected Version(s): From (including) 6.8 Up to (excluding) 6.10.3					
Allocation of Resources Without Limits or Throttling	12-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm: huge_memory: use !CONFIG_64BIT to relax huge page alignment on 32 bit machines	https://git.kernel.org/stable/c/7e1f4efb8d6140b2ec79bf760c43e1fc186e8dfc, https://git.kernel.org/stable/c/d9592025000b3cf26c742f3505da7b83aedc26d5	O-LIN-LINU-080824/2143

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Yves-Alexis Perez reported commit 4ef9ad19e176 ("mm: huge_memory: don't force huge page alignment on 32 bit") didn't work for x86_32 [1]. It is because x86_32 uses CONFIG_X86_32 instead of CONFIG_32BIT. !CONFIG_64BIT should cover all 32 bit machines. [1] https://lore.kernel.org/linux-mm/CAHbLzkr1LwH3pcTgM+aGQ31ip2bKqiqEQ8=FQB+t2c3dhNKNHA@mail.gmail.com/ **CVE ID: CVE-2024-42258**		
Affected Version(s): From (including) 6.8 Up to (excluding) 6.9.10					
Improper Locking	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: cachefiles: add missing lock	https://git.kernel.org/stable/c/6bb6bd3dd6f382dfd36220d4b210a0c77c066651, https://git.kernel.org/stable/c/8eadcab7f3dd8	O-LIN-LINU-080824/2144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protection when polling Add missing lock protection in poll routine when iterating xarray, otherwise: Even with RCU read lock held, only the slot of the radix tree is ensured to be pinned there, while the data structure (e.g. struct cachefiles_req) stored in the slot has no such guarantee. The poll routine will iterate the radix tree and dereference cachefiles_req accordingly. Thus RCU read lock is not adequate in this case and spinlock is needed here. **CVE ID: CVE-2024-42250**	09edbe5ae20533ff843dfea3a07, https://git.kernel.org/stable/c/97cfd5e20ddc2e33e16ce369626ce76c9a475fd7	
Affected Version(s): From (including) 6.9 Up to (excluding) 6.9.10					
Allocation of Resources Without	07-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/63d20a94f24fc1cbaf44d0e7c0e0a8077fde0aef,	O-LIN-LINU-080824/2145

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

Limits or Throttling			mmc: sdhci: Fix max_seg_size for 64KiB PAGE_SIZE
			
			blk_queue_max_segment_size() ensured:
			
			if (max_size < PAGE_SIZE)
			
			max_size = PAGE_SIZE;
			
			whereas:
			
			blk_validate_limits() makes it an error:
			
			if (WARN_ON_ONCE(lim->max_segment_size < PAGE_SIZE))
			
			return -EINVAL;
			
			The change from one to the other, exposed sdhci which was setting maximum
			segment size too low in some circumstances.
				https://git.kernel.org/stable/c/bf78b1accef46efd9b624967cb74ae8d3c215a2b	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fix the maximum segment size when it is too low. **CVE ID: CVE-2024-42242**		
N/A	07-Aug-2024	3.3	In the Linux kernel, the following vulnerability has been resolved: filemap: replace pte_offset_map() with pte_offset_map_nolock() The vmf->ptl in filemap_fault_recheck_pte_none() is still set from handle_pte_fault(). But at the same time, we did a pte_unmap(vmf->pte). After a pte_unmap(vmf->pte) unmap and rcu_read_unlock(), the page table may be racily changed and vmf->ptl maybe fails to protect the actual page table. Fix this by replacing pte_offset_map() with	https://git.kernel.org/stable/c/24be02a42181f0707be0498045c4c4b13273b16d, https://git.kernel.org/stable/c/6a6c2aec1a89506595801b4cf7e8eef035f33748	O-LIN-LINU-080824/2146

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pte_offset_map_nolock(). As David said, the PTL pointer might be stale so if we continue to use it infilemap_fault_recheck_pte_none(), it might trigger UAF. Also, if the PTL fails, the issue fixed by commit 58f327f2ce80 ("filemap: avoid unnecessary major faults in filemap_fault()") might reappear. **CVE ID: CVE-2024-42233**		
N/A	07-Aug-2024	3.3	In the Linux kernel, the following vulnerability has been resolved: spi: don't unoptimize message in spi_async() Calling spi_maybe_unoptimize_message() in spi_async() is wrong because the message is likely to be in the	https://git.kernel.org/stable/c/8b9af6d67517ce4a0015928b3cf35bfd2b1bc1c2, https://git.kernel.org/stable/c/c86a918b1bdba78fb155184f8d88dfba1e63335d	O-LIN-LINU-080824/2147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			queue and not transferred yet. This can corrupt the message while it is being used by the controller driver. spi_maybe_unoptimize_message() is already called in the correct place in spi_finalize_current_message() to balance the call to spi_maybe_optimize_message() in spi_async(). **CVE ID: CVE-2024-42249**		
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Use After Free	14-Aug-2024	7.8	Photoshop Desktop versions 24.7.3, 25.9.1 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/photoshop/apsb24-49.html	O-MIC-WIND-080824/2148

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-34117		
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41831**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-MIC-WIND-080824/2149
Out-of-bounds Write	14-Aug-2024	7.8	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41840**	https://helpx.adobe.com/security/products/bridge/apsb24-59.html	O-MIC-WIND-080824/2150

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	14-Aug-2024	7.8	Illustrator versions 28.5, 27.9.4 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-2024-34133**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-MIC-WIND-080824/2151
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41850**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-MIC-WIND-080824/2152
Out-of-bounds Write	14-Aug-2024	7.8	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds write vulnerability that	https://helpx.adobe.com/security/products/bridge/apsb24-59.html	O-MIC-WIND-080824/2153

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39386**		
Integer Overflow or Wraparound	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41851**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-MIC-WIND-080824/2154
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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.	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-MIC-WIND-080824/2155

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41852**		
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41853**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-MIC-WIND-080824/2156
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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/apsb24-57.html	O-MIC-WIND-080824/2157

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-39383**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Aug-2024	7.8	Improper path validation in promecefpluginhost.exe in Kingsoft WPS Office version ranging from 12.2.0.13110 to 12.2.0.17115 (exclusive) on Windows allows an attacker to load an arbitrary Windows library. The patch released in version 12.1.0.17119 to mitigate CVE-2024-7262 was not restrictive enough. Another parameter was not properly sanitized which leads to the execution of an arbitrary Windows library. **CVE ID: CVE-2024-7263**	https://www.wps.com/whatsnew/pc/20240422/	O-MIC-WIND-080824/2158
N/A	14-Aug-2024	7.8	Illustrator versions 28.5, 27.9.4 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-MIC-WIND-080824/2159

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41856**		
Use After Free	14-Aug-2024	7.8	Substance3D - Stager versions 3.0.2 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-2024-39388**	N/A	O-MIC-WIND-080824/2160
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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/indesign/apsb24-56.html	O-MIC-WIND-080824/2161

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-39389**		
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-39390**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-MIC-WIND-080824/2162
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-39391**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-MIC-WIND-080824/2163

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39393**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-MIC-WIND-080824/2164
Out-of-bounds Write	14-Aug-2024	7.8	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-39394**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-MIC-WIND-080824/2165

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Aug-2024	7.8	webcrack is a tool for reverse engineering javascript. An arbitrary file write vulnerability exists in the webcrack module when processing specifically crafted malicious code on Windows systems. This vulnerability is triggered when using the unpack bundles feature in conjunction with the saving feature. If a module name includes a path traversal sequence with Windows path separators, an attacker can exploit this to overwrite files on the host system. This vulnerability allows an attacker to write arbitrary `.js` files to the host system, which can be leveraged to hijack legitimate Node.js modules to gain arbitrary code execution. This vulnerability has been patched in version 2.14.1. **CVE ID: CVE-2024-43373**	https://github.com/j4k0xb/webcrack/commit/4bc5c6f353012ee7edc2cb39d01a728ab7426999, https://github.com/j4k0xb/webcrack/security/advisories/GHSA-ccqh-278p-xq6w	O-MIC-WIND-080824/2166

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Aug-2024	7.8	Improper path validation in promecefpluginhost.exe in Kingsoft WPS Office version ranging from 12.2.0.13110 to 12.2.0.16412 (exclusive) on Windows allows an attacker to load an arbitrary Windows library. The vulnerability was found weaponized as a single-click exploit in the form of a deceptive spreadsheet document **CVE ID: CVE-2024-7262**	https://www.wps.com/whatsnew/pc/20240422/	O-MIC-WIND-080824/2167
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-MIC-WIND-080824/2168

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39422		
Out-of-bounds Write	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-39423**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-MIC-WIND-080824/2169
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-MIC-WIND-080824/2170

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39424		
Out-of-bounds Read	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39426**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-MIC-WIND-080824/2171
Use After Free	14-Aug-2024	7.8	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-MIC-WIND-080824/2172

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41830**		
Out-of-bounds Read	14-Aug-2024	7.1	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-34127**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-MIC-WIND-080824/2173
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could result in	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-MIC-WIND-080824/2174

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. This issue occurs when the state of a resource changes between its check-time and use-time, allowing an attacker to manipulate the resource. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39420**		
Time-of-check Time-of-use (TOCTOU) Race Condition	14-Aug-2024	7	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to privilege escalation. Exploitation of this issue require local low-privilege access to the affected system and attack complexity is high.	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-MIC-WIND-080824/2175

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39425		
N/A	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by an Improper Input Validation vulnerability that could lead to an application denial-of-service condition. An attacker could exploit this vulnerability to render the application unresponsive or terminate its execution. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34118**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-MIC-WIND-080824/2176
Out-of-bounds Read	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 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/illustrator/apsb24-45.html	O-MIC-WIND-080824/2177

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34134**		
NULL Pointer Dereference	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34136**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-MIC-WIND-080824/2178
NULL Pointer Dereference	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS) condition. An attacker could exploit this vulnerability to crash the	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-MIC-WIND-080824/2179

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application, resulting in a DoS. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34137**		
NULL Pointer Dereference	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34138**	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-MIC-WIND-080824/2180
Out-of-bounds Read	14-Aug-2024	5.5	Illustrator versions 28.5, 27.9.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could	https://helpx.adobe.com/security/products/illustrator/apsb24-45.html	O-MIC-WIND-080824/2181

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-34135**		
Out-of-bounds Read	14-Aug-2024	5.5	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39387**	https://helpx.adobe.com/security/products/bridge/apsb24-59.html	O-MIC-WIND-080824/2182
NULL Pointer Dereference	14-Aug-2024	5.5	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-MIC-WIND-080824/2183

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability to crash the application, resulting in a DoS condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39395**		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41835**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-MIC-WIND-080824/2184
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964,	https://helpx.adobe.com/security/products/ac	O-MIC-WIND-080824/2185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			24.001.30123 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-2024-41832**	robat/apsb24-57.html	
NULL Pointer Dereference	14-Aug-2024	5.5	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-MIC-WIND-080824/2186

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41866		
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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-2024-41833**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-MIC-WIND-080824/2187
Out-of-bounds Read	14-Aug-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-MIC-WIND-080824/2188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41834**		
Out-of-bounds Read	14-Aug-2024	5.5	InDesign Desktop versions ID19.4, ID18.5.2 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-2024-41854**	https://helpx.adobe.com/security/products/indesign/apsb24-56.html	O-MIC-WIND-080824/2189
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.20680					
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2190
Affected Version(s): * Up to (excluding) 10.0.10240.20751					
N/A	13-Aug-2024	9.8	Windows Reliable Multicast	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2191

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	date-guide/vulnerability/CVE-2024-38140	
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2192
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2193
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2194
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2195
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2196

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID: CVE-2024-38114**	lity/CVE-2024-38114	
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2197
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2198
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2199
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2200
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2201

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-29995	lity/CVE-2024-29995	
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38107**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107	O-MIC-WIND-080824/2202
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2203
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2204
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2205
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38142**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38142	O-MIC-WIND-080824/2206

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2207
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2208
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2209
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2210
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2211
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2212

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2213
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2214
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2215
N/A	13-Aug-2024	7.5	Scripting Engine Memory Corruption Vulnerability **CVE ID: CVE-2024-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178	O-MIC-WIND-080824/2216
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2217
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2218

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2219
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2220
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2221
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2222
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2223
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2224

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38143**	lity/CVE-2024-38143	
Product: windows_10_1607					
Affected Version(s): * Up to (excluding) 10.0.14393.7070					
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2225
Affected Version(s): * Up to (excluding) 10.0.14393.7159					
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38184	O-MIC-WIND-080824/2226
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38185**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38185	O-MIC-WIND-080824/2227
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38186	O-MIC-WIND-080824/2228
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2229

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38187	lity/CVE-2024-38187	
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2230
Affected Version(s): * Up to (excluding) 10.0.14393.7259					
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2231
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2232
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2233
N/A	13-Aug-2024	9.1	Windows Network Virtualization Remote Code Execution Vulnerability **CVE ID: CVE-2024-38160**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38160	O-MIC-WIND-080824/2234

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	9.1	Windows Network Virtualization Remote Code Execution Vulnerability **CVE ID: CVE-2024-38159**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38159	O-MIC-WIND-080824/2235
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2236
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2237
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2238
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2239

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2240
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2241
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2242
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID: CVE-2024-29995**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29995	O-MIC-WIND-080824/2243
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38107**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107	O-MIC-WIND-080824/2244
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2245

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38117	lity/CVE-2024-38117	
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2246
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2247
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2248
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2249
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38142**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38142	O-MIC-WIND-080824/2250
N/A	13-Aug-2024	7.8	Windows OLE Remote Code	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2251

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38152**	date-guide/vulnerability/CVE-2024-38152	
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2252
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2253
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2254
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2255
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2256
N/A	13-Aug-2024	7.5	Scripting Engine Memory	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2257

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Corruption Vulnerability **CVE ID: CVE-2024-38178**	date-guide/vulnerability/CVE-2024-38178	
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2258
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2259
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2260
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2261
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2262
N/A	13-Aug-2024	5.5	Windows Kernel Information	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2263

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID: CVE-2024-38151**	date-guide/vulnerability/CVE-2024-38151	
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2264
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2265
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143	O-MIC-WIND-080824/2266
Product: windows_10_1809					
Affected Version(s): * Up to (excluding) 10.0.17763.5936					
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2267
Affected Version(s): * Up to (excluding) 10.0.17763.6054					
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2268

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38184**	guide/vulnerability/CVE-2024-38184	
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38185**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38185	O-MIC-WIND-080824/2269
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38186	O-MIC-WIND-080824/2270
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38187**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38187	O-MIC-WIND-080824/2271
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2272
N/A	13-Aug-2024	6.8	Windows Mobile Broadband Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38161**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38161	O-MIC-WIND-080824/2273
Affected Version(s): * Up to (excluding) 10.0.17763.6189					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2274
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2275
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2276
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2277
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2278
N/A	13-Aug-2024	8.8	Windows IP Routing Management	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2279

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	guide/vulnerability/CVE-2024-38115	
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2280
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2281
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2282
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2283
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2284

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-29995	lity/CVE-2024-29995	
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38107**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107	O-MIC-WIND-080824/2285
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2286
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2287
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2288
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2289
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2290

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38142**	lity/CVE-2024-38142	
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2291
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2292
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2293
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2294
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2295
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2296

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38133**	date-guide/vulnerability/CVE-2024-38133	
N/A	13-Aug-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38215**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38215	O-MIC-WIND-080824/2297
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2298
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2299
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2300
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2301

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.5	Scripting Engine Memory Corruption Vulnerability **CVE ID: CVE-2024-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178	O-MIC-WIND-080824/2302
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2303
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2304
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38136**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38136	O-MIC-WIND-080824/2305
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2306
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID: CVE-2024-38118**	lity/CVE-2024-38118	
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2308
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2309
N/A	13-Aug-2024	5.5	Security Center Broker Information Disclosure Vulnerability **CVE ID: CVE-2024-38155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38155	O-MIC-WIND-080824/2310
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143	O-MIC-WIND-080824/2311
Product: windows_10_21h2					
Affected Version(s): * Up to (excluding) 10.0.19044.4529					
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2312

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 10.0.19044.4651					
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38184	O-MIC-WIND-080824/2313
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38185**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38185	O-MIC-WIND-080824/2314
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38186	O-MIC-WIND-080824/2315
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38187**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38187	O-MIC-WIND-080824/2316
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2317
N/A	13-Aug-2024	6.8	Windows Mobile Broadband Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38161**	lity/CVE-2024-38161	
Affected Version(s): * Up to (excluding) 10.0.19044.4780					
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2319
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2320
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2321
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2322
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2323

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38144		
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2324
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2325
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2326
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2327
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2328

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38131		
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID: CVE-2024-29995**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29995	O-MIC-WIND-080824/2329
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38107**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107	O-MIC-WIND-080824/2330
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2331
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2332
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2333
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2334

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38133	lity/CVE-2024-38133	
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2335
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38142**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38142	O-MIC-WIND-080824/2336
N/A	13-Aug-2024	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38147**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38147	O-MIC-WIND-080824/2337
N/A	13-Aug-2024	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38150**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38150	O-MIC-WIND-080824/2338
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2339
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2340

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38153	lity/CVE-2024-38153	
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2341
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2342
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2343
N/A	13-Aug-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38215**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38215	O-MIC-WIND-080824/2344
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2345
N/A	13-Aug-2024	7.5	Windows Network Address	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2346

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	date-guide/vulnerability/CVE-2024-38132	
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2347
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2348
N/A	13-Aug-2024	7.5	Scripting Engine Memory Corruption Vulnerability **CVE ID: CVE-2024-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178	O-MIC-WIND-080824/2349
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2350
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2351
Concurrent Execution using	13-Aug-2024	7	Windows Resource Manager PSM Service Extension	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38137**	guide/vulnerability/CVE-2024-38137	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38136**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38136	O-MIC-WIND-080824/2353
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2354
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2355
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2356

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38122		
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2357
N/A	13-Aug-2024	5.5	Security Center Broker Information Disclosure Vulnerability **CVE ID: CVE-2024-38155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38155	O-MIC-WIND-080824/2358
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143	O-MIC-WIND-080824/2359
Product: windows_10_22h2					
Affected Version(s): * Up to (excluding) 10.0.19045.4529					
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2360
Affected Version(s): * Up to (excluding) 10.0.19045.4651					
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38184	O-MIC-WIND-080824/2361
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38185**	date-guide/vulnerability/CVE-2024-38185	
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38186	O-MIC-WIND-080824/2363
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38187**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38187	O-MIC-WIND-080824/2364
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2365
N/A	13-Aug-2024	6.8	Windows Mobile Broadband Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38161**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38161	O-MIC-WIND-080824/2366
Affected Version(s): * Up to (excluding) 10.0.19045.4780					
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2367

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38140		
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2368
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2369
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2370
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2371
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2372

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2373
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2374
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2375
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2376
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID: CVE-2024-29995**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29995	O-MIC-WIND-080824/2377
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2378

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38107**	lity/CVE-2024-38107	
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2379
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2380
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2381
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38133**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38133	O-MIC-WIND-080824/2382
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2383
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38142**	guide/vulnerability/CVE-2024-38142	
N/A	13-Aug-2024	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38147**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38147	O-MIC-WIND-080824/2385
N/A	13-Aug-2024	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38150**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38150	O-MIC-WIND-080824/2386
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2387
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2388
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2389
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38196**	guide/vulnerability/CVE-2024-38196	
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2391
N/A	13-Aug-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38215**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38215	O-MIC-WIND-080824/2392
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2393
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2394
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2395

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2396
N/A	13-Aug-2024	7.5	Scripting Engine Memory Corruption Vulnerability **CVE ID: CVE-2024-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178	O-MIC-WIND-080824/2397
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2398
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2399
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38137**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38137	O-MIC-WIND-080824/2400
Concurrent Execution using Shared Resource	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2401

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			Privilege Vulnerability **CVE ID: CVE-2024-38136**	lity/CVE-2024-38136	
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2402
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2403
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2404
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2405
N/A	13-Aug-2024	5.5	Security Center Broker Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2406

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38155	lity/CVE-2024-38155	
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143	O-MIC-WIND-080824/2407
Product: windows_11_21h2					
Affected Version(s): * Up to (excluding) 10.0.22000.3019					
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2408
Affected Version(s): * Up to (excluding) 10.0.22000.3079					
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38184	O-MIC-WIND-080824/2409
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38185**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38185	O-MIC-WIND-080824/2410
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38186	O-MIC-WIND-080824/2411

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38187**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38187	O-MIC-WIND-080824/2412
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2413
N/A	13-Aug-2024	6.8	Windows Mobile Broadband Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38161**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38161	O-MIC-WIND-080824/2414
Affected Version(s): * Up to (excluding) 10.0.22000.3147					
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2415
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2416
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2417

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38199**	lity/CVE-2024-38199	
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2418
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2419
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2420
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2421
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2422

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38130**	lity/CVE-2024-38130	
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2423
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2424
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID: CVE-2024-29995**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29995	O-MIC-WIND-080824/2425
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2426
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38107**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107	O-MIC-WIND-080824/2427

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2428
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2429
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2430
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2431
N/A	13-Aug-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38215**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38215	O-MIC-WIND-080824/2432
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2433

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38127		
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38133**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38133	O-MIC-WIND-080824/2434
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2435
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2436
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38142**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38142	O-MIC-WIND-080824/2437
N/A	13-Aug-2024	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38147**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38147	O-MIC-WIND-080824/2438
N/A	13-Aug-2024	7.8	Windows DWM Core Library Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38150**	guide/vulnerability/CVE-2024-38150	
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2440
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2441
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2442
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2443
N/A	13-Aug-2024	7.5	Scripting Engine Memory Corruption Vulnerability **CVE ID: CVE-2024-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178	O-MIC-WIND-080824/2444
N/A	13-Aug-2024	7.5	Windows Secure Channel Denial of	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2445

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service Vulnerability **CVE ID: CVE-2024-38148**	guide/vulnerability/CVE-2024-38148	
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2446
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2447
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2448
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38136**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38136	O-MIC-WIND-080824/2449
Concurrent Execution using Shared Resource with Improper	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38137	O-MIC-WIND-080824/2450

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			**CVE ID: CVE-2024-38137**		
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2451
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2452
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2453
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2454
N/A	13-Aug-2024	5.5	Security Center Broker Information Disclosure Vulnerability **CVE ID: CVE-2024-38155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38155	O-MIC-WIND-080824/2455

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143	O-MIC-WIND-080824/2456
Product: windows_11_22h2					
Affected Version(s): * Up to (excluding) 10.0.22621.3737					
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2457
Affected Version(s): * Up to (excluding) 10.0.22621.3880					
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38184	O-MIC-WIND-080824/2458
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38185**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38185	O-MIC-WIND-080824/2459
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38186	O-MIC-WIND-080824/2460
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2461

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38187**	date-guide/vulnerability/CVE-2024-38187	
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2462
N/A	13-Aug-2024	6.8	Windows Mobile Broadband Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38161**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38161	O-MIC-WIND-080824/2463
N/A	13-Aug-2024	6.5	Windows Compressed Folder Tampering Vulnerability **CVE ID: CVE-2024-38165**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38165	O-MIC-WIND-080824/2464
Affected Version(s): * Up to (excluding) 10.0.22621.4037					
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2465
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2466

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2467
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2468
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2469
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2470
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2471

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2472
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2473
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2474
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID: CVE-2024-29995**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29995	O-MIC-WIND-080824/2475
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2476
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2477

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38107**	lity/CVE-2024-38107	
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2478
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2479
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2480
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2481
N/A	13-Aug-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38215**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38215	O-MIC-WIND-080824/2482

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2483
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2484
N/A	13-Aug-2024	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38135**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38135	O-MIC-WIND-080824/2485
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38133**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38133	O-MIC-WIND-080824/2486
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2487
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38142	O-MIC-WIND-080824/2488

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38142		
N/A	13-Aug-2024	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38147**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38147	O-MIC-WIND-080824/2489
N/A	13-Aug-2024	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38150**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38150	O-MIC-WIND-080824/2490
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2491
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2492
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2493
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2494

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service Vulnerability **CVE ID: CVE-2024-38146**	lity/CVE-2024-38146	
N/A	13-Aug-2024	7.5	Scripting Engine Memory Corruption Vulnerability **CVE ID: CVE-2024-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178	O-MIC-WIND-080824/2495
N/A	13-Aug-2024	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID: CVE-2024-38148**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38148	O-MIC-WIND-080824/2496
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2497
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2498
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2499
Concurrent Execution using Shared Resource	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2500

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			Privilege Vulnerability **CVE ID: CVE-2024-38136**	lity/CVE-2024-38136	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38137**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38137	O-MIC-WIND-080824/2501
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2502
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2503
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2504

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2505
N/A	13-Aug-2024	5.5	Security Center Broker Information Disclosure Vulnerability **CVE ID: CVE-2024-38155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38155	O-MIC-WIND-080824/2506
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143	O-MIC-WIND-080824/2507
Product: windows_11_23h2					
Affected Version(s): * Up to (excluding) 10.0.22631.3737					
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2508
Affected Version(s): * Up to (excluding) 10.0.22631.3880					
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38184	O-MIC-WIND-080824/2509
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38185**	lity/CVE-2024-38185	
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38186	O-MIC-WIND-080824/2511
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38187**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38187	O-MIC-WIND-080824/2512
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2513
N/A	13-Aug-2024	6.8	Windows Mobile Broadband Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38161**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38161	O-MIC-WIND-080824/2514
N/A	13-Aug-2024	6.5	Windows Compressed Folder Tampering Vulnerability **CVE ID: CVE-2024-38165**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38165	O-MIC-WIND-080824/2515
Affected Version(s): * Up to (excluding) 10.0.22631.4037					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2516
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2517
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2518
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2519
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2520
N/A	13-Aug-2024	8.8	Windows IP Routing Management	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2521

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	guide/vulnerability/CVE-2024-38115	
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2522
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2523
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2524
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2525
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2526

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38153	lity/CVE-2024-38153	
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38107**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107	O-MIC-WIND-080824/2527
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2528
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2529
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2530
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2531
N/A	13-Aug-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2532

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38215**	guide/vulnerability/CVE-2024-38215	
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2533
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38133**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38133	O-MIC-WIND-080824/2534
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2535
N/A	13-Aug-2024	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38135**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38135	O-MIC-WIND-080824/2536
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2537
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2538

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38142**	date-guide/vulnerability/CVE-2024-38142	
N/A	13-Aug-2024	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38147**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38147	O-MIC-WIND-080824/2539
N/A	13-Aug-2024	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38150**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38150	O-MIC-WIND-080824/2540
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2541
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2542
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2543

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2544
N/A	13-Aug-2024	7.5	Scripting Engine Memory Corruption Vulnerability **CVE ID: CVE-2024-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178	O-MIC-WIND-080824/2545
N/A	13-Aug-2024	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID: CVE-2024-38148**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38148	O-MIC-WIND-080824/2546
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2547
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2548
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2549
Concurrent Execution	13-Aug-2024	7	Windows Resource Manager PSM	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2550

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38136**	date-guide/vulnerability/CVE-2024-38136	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38137**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38137	O-MIC-WIND-080824/2551
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2552
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2553
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2554

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38122		
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2555
N/A	13-Aug-2024	5.5	Security Center Broker Information Disclosure Vulnerability **CVE ID: CVE-2024-38155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38155	O-MIC-WIND-080824/2556
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143	O-MIC-WIND-080824/2557
Product: windows_11_24h2					
Affected Version(s): * Up to (excluding) 10.0.26100.1457					
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2558
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2559
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2560

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	date-guide/vulnerability/CVE-2024-38199	
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2561
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2562
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2563
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2564
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2565

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID: CVE-2024-38116**	lity/CVE-2024-38116	
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2566
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2567
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2568
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38107**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107	O-MIC-WIND-080824/2569
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2570

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2571
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38184	O-MIC-WIND-080824/2572
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2573
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2574
N/A	13-Aug-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38215**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38215	O-MIC-WIND-080824/2575
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2576

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38127	lity/CVE-2024-38127	
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38133**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38133	O-MIC-WIND-080824/2577
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2578
N/A	13-Aug-2024	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38135**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38135	O-MIC-WIND-080824/2579
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2580
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38142**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38142	O-MIC-WIND-080824/2581
N/A	13-Aug-2024	7.8	Microsoft DWM Core Library Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38147**	guide/vulnerability/CVE-2024-38147	
N/A	13-Aug-2024	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38150**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38150	O-MIC-WIND-080824/2583
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2584
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2585
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2586
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2587
N/A	13-Aug-2024	7.5	Scripting Engine Memory	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2588

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Corruption Vulnerability **CVE ID: CVE-2024-38178**	date-guide/vulnerability/CVE-2024-38178	
N/A	13-Aug-2024	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID: CVE-2024-38148**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38148	O-MIC-WIND-080824/2589
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2590
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2591
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2592
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38136**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38136	O-MIC-WIND-080824/2593

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38137**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38137	O-MIC-WIND-080824/2594
N/A	13-Aug-2024	6.8	Windows Mobile Broadband Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38161**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38161	O-MIC-WIND-080824/2595
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2596
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2597
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2598

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38122		
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2599
N/A	13-Aug-2024	5.5	Security Center Broker Information Disclosure Vulnerability **CVE ID: CVE-2024-38155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38155	O-MIC-WIND-080824/2600
N/A	13-Aug-2024	4.4	Windows Bluetooth Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38123**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38123	O-MIC-WIND-080824/2601
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143	O-MIC-WIND-080824/2602
Product: windows_server_2008					
Affected Version(s): -					
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2603
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2604

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	guide/vulnerability/CVE-2024-38140	
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2605
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2606
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2607
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2608
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2609

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38120**	lity/CVE-2024-38120	
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38121**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38121	O-MIC-WIND-080824/2610
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38128**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38128	O-MIC-WIND-080824/2611
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2612
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2613
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2614

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38144**	lity/CVE-2024-38144	
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38154	O-MIC-WIND-080824/2615
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2616
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID: CVE-2024-29995**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29995	O-MIC-WIND-080824/2617
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2618
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2619

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2620
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2621
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2622
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2623
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2624
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2625

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38196		
N/A	13-Aug-2024	7.5	Windows DNS Spoofing Vulnerability **CVE ID: CVE-2024-37968**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37968	O-MIC-WIND-080824/2626
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2627
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2628
N/A	13-Aug-2024	6.5	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability **CVE ID: CVE-2024-38214**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38214	O-MIC-WIND-080824/2629
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2630

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2631
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2632
Affected Version(s): r2					
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2633
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2634
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2635
N/A	13-Aug-2024	8.8	Windows IP Routing Management	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2636

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	guide/vulnerability/CVE-2024-38114	
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2637
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2638
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38120**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38120	O-MIC-WIND-080824/2639
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38121**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38121	O-MIC-WIND-080824/2640
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2641

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38128**	lity/CVE-2024-38128	
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2642
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2643
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2644
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38154	O-MIC-WIND-080824/2645
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2646

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38180	lity/CVE-2024-38180	
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID: CVE-2024-29995**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29995	O-MIC-WIND-080824/2647
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2648
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2649
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2650
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2651
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2652

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38152	lity/CVE-2024-38152	
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2653
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2654
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2655
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2656
N/A	13-Aug-2024	7.5	Windows DNS Spoofing Vulnerability **CVE ID: CVE-2024-37968**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37968	O-MIC-WIND-080824/2657
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2658

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38198	lity/CVE-2024-38198	
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2659
N/A	13-Aug-2024	6.5	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability **CVE ID: CVE-2024-38214**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38214	O-MIC-WIND-080824/2660
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2661
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2662
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2663

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows_server_2012					
Affected Version(s): r2					
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2664
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2665
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2666
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38128**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38128	O-MIC-WIND-080824/2667
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2668

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2669
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2670
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2671
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2672
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38120**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38120	O-MIC-WIND-080824/2673

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38121**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38121	O-MIC-WIND-080824/2674
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38154	O-MIC-WIND-080824/2675
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2676
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2677
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID: CVE-2024-29995**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29995	O-MIC-WIND-080824/2678
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2679

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38107**	lity/CVE-2024-38107	
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2680
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2681
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2682
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2683
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2684

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2685
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2686
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2687
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2688
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2689
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2690

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2691
N/A	13-Aug-2024	7.5	Scripting Engine Memory Corruption Vulnerability **CVE ID: CVE-2024-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178	O-MIC-WIND-080824/2692
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2693
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2694
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2695
N/A	13-Aug-2024	7.5	Windows DNS Spoofing Vulnerability **CVE ID: CVE-2024-37968**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37968	O-MIC-WIND-080824/2696

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2697
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2698
N/A	13-Aug-2024	6.5	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability **CVE ID: CVE-2024-38214**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38214	O-MIC-WIND-080824/2699
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2700
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2701
N/A	13-Aug-2024	5.5	Windows Kernel Information	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2702

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID: CVE-2024-38151**	guide/vulnerability/CVE-2024-38151	
Affected Version(s): * Up to (excluding) 6.2.9200.24919					
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2703
Affected Version(s): * Up to (excluding) 6.2.9200.24975					
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2704
Affected Version(s): * Up to (excluding) 6.2.9200.25031					
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2705
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2706
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2707

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID: CVE-2024-38140**	lity/CVE-2024-38140	
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2708
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38128**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38128	O-MIC-WIND-080824/2709
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2710
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2711
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2712

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID: CVE-2024-38115**	lity/CVE-2024-38115	
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2713
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2714
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38120**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38120	O-MIC-WIND-080824/2715
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38121**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38121	O-MIC-WIND-080824/2716
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2717

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38154**	lity/CVE-2024-38154	
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2718
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID: CVE-2024-29995**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29995	O-MIC-WIND-080824/2719
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38107**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107	O-MIC-WIND-080824/2720
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2721
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2722

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2723
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2724
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2725
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2726
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2727
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2728

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.5	Windows DNS Spoofing Vulnerability **CVE ID: CVE-2024-37968**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37968	O-MIC-WIND-080824/2729
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2730
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2731
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2732
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2733
N/A	13-Aug-2024	6.5	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38214	O-MIC-WIND-080824/2734

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38214		
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2735
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2736
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2737
Product: windows_server_2016					
Affected Version(s): * Up to (excluding) 10.0.14393.7070					
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2738
Affected Version(s): * Up to (excluding) 10.0.14393.7159					
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38184	O-MIC-WIND-080824/2739

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38184		
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38185**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38185	O-MIC-WIND-080824/2740
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38186	O-MIC-WIND-080824/2741
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38187**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38187	O-MIC-WIND-080824/2742
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2743
Affected Version(s): * Up to (excluding) 10.0.14393.7259					
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2744

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2745
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2746
N/A	13-Aug-2024	9.1	Windows Network Virtualization Remote Code Execution Vulnerability **CVE ID: CVE-2024-38159**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38159	O-MIC-WIND-080824/2747
N/A	13-Aug-2024	9.1	Windows Network Virtualization Remote Code Execution Vulnerability **CVE ID: CVE-2024-38160**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38160	O-MIC-WIND-080824/2748
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2749
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2750

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38154**	lity/CVE-2024-38154	
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2751
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38128**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38128	O-MIC-WIND-080824/2752
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38120**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38120	O-MIC-WIND-080824/2753
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2754
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2755

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID: CVE-2024-38116**	lity/CVE-2024-38116	
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2756
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2757
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2758
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38121**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38121	O-MIC-WIND-080824/2759
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2760

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-29995	lity/CVE-2024-29995	
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38107**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107	O-MIC-WIND-080824/2761
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2762
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2763
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38142**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38142	O-MIC-WIND-080824/2764
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2765
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2766

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38153**	lity/CVE-2024-38153	
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2767
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2768
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2769
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2770
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2771

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.5	Windows DNS Spoofing Vulnerability **CVE ID: CVE-2024-37968**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37968	O-MIC-WIND-080824/2772
N/A	13-Aug-2024	7.5	Windows Deployment Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-38138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38138	O-MIC-WIND-080824/2773
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2774
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2775
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2776
N/A	13-Aug-2024	7.5	Scripting Engine Memory Corruption Vulnerability **CVE ID: CVE-2024-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178	O-MIC-WIND-080824/2777

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2778
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2779
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2780
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2781
N/A	13-Aug-2024	6.5	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability **CVE ID: CVE-2024-38214**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38214	O-MIC-WIND-080824/2782
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2783

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID: CVE-2024-38118**	lity/CVE-2024-38118	
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2784
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2785
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143	O-MIC-WIND-080824/2786
Product: windows_server_2019					
Affected Version(s): * Up to (excluding) 10.0.17763.5936					
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2787
Affected Version(s): * Up to (excluding) 10.0.17763.6054					
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2788

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38184	lity/CVE-2024-38184	
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38185**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38185	O-MIC-WIND-080824/2789
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38186	O-MIC-WIND-080824/2790
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38187**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38187	O-MIC-WIND-080824/2791
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2792
N/A	13-Aug-2024	6.8	Windows Mobile Broadband Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38161**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38161	O-MIC-WIND-080824/2793
Affected Version(s): * Up to (excluding) 10.0.17763.6189					
N/A	13-Aug-2024	9.8	Windows Reliable Multicast	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2794

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	date-guide/vulnerability/CVE-2024-38140	
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2795
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2796
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2797
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38128**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38128	O-MIC-WIND-080824/2798
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2799

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38120**	lity/CVE-2024-38120	
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2800
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2801
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2802
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2803
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2804

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38121**	lity/CVE-2024-38121	
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38154	O-MIC-WIND-080824/2805
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2806
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2807
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID: CVE-2024-29995**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29995	O-MIC-WIND-080824/2808
N/A	13-Aug-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38215**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38215	O-MIC-WIND-080824/2809

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38107**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107	O-MIC-WIND-080824/2810
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2811
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2812
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2813
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38133**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38133	O-MIC-WIND-080824/2814
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2815

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38134		
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2816
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2817
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38142**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38142	O-MIC-WIND-080824/2818
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2819
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2820
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2821

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38193	lity/CVE-2024-38193	
N/A	13-Aug-2024	7.5	Windows DNS Spoofing Vulnerability **CVE ID: CVE-2024-37968**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37968	O-MIC-WIND-080824/2822
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2823
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2824
N/A	13-Aug-2024	7.5	Windows Deployment Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-38138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38138	O-MIC-WIND-080824/2825
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2826
N/A	13-Aug-2024	7.5	Scripting Engine Memory Corruption Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38178	lity/CVE-2024-38178	
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2828
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2829
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38136**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38136	O-MIC-WIND-080824/2830
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2831
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2832

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	6.5	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability **CVE ID: CVE-2024-38214**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38214	O-MIC-WIND-080824/2833
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2834
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2835
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2836
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143	O-MIC-WIND-080824/2837
Product: windows_server_2022					
Affected Version(s): * Up to (excluding) 10.0.20348.2522					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2838
Affected Version(s): * Up to (excluding) 10.0.20348.2582					
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38184	O-MIC-WIND-080824/2839
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38185**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38185	O-MIC-WIND-080824/2840
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38186	O-MIC-WIND-080824/2841
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38187**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38187	O-MIC-WIND-080824/2842
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2843

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38191	lity/CVE-2024-38191	
Affected Version(s): * Up to (excluding) 10.0.20348.2655					
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability **CVE ID: CVE-2024-38063**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063	O-MIC-WIND-080824/2844
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2845
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2846
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38115**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2847
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2848

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38114		
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2849
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2850
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38120**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38120	O-MIC-WIND-080824/2851
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38121**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38121	O-MIC-WIND-080824/2852
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38128	O-MIC-WIND-080824/2853

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38128		
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38130**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2854
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2855
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38154	O-MIC-WIND-080824/2856
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2857
N/A	13-Aug-2024	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID: CVE-2024-29995**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29995	O-MIC-WIND-080824/2858

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2859
N/A	13-Aug-2024	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38147**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38147	O-MIC-WIND-080824/2860
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38107**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107	O-MIC-WIND-080824/2861
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2862
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38142**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38142	O-MIC-WIND-080824/2863
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2864

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38125**	lity/CVE-2024-38125	
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2865
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2866
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38133**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38133	O-MIC-WIND-080824/2867
N/A	13-Aug-2024	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38150**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38150	O-MIC-WIND-080824/2868
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2869
N/A	13-Aug-2024	7.8	Windows OLE Remote Code	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2870

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38152**	guide/vulnerability/CVE-2024-38152	
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38153	O-MIC-WIND-080824/2871
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2872
N/A	13-Aug-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38215**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38215	O-MIC-WIND-080824/2873
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2874
N/A	13-Aug-2024	7.5	Windows Deployment Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-38138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38138	O-MIC-WIND-080824/2875
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network	https://msrc.microsoft.com/up	O-MIC-WIND-080824/2876

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	date-guide/vulnerability/CVE-2024-38145	
N/A	13-Aug-2024	7.5	Scripting Engine Memory Corruption Vulnerability **CVE ID: CVE-2024-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178	O-MIC-WIND-080824/2877
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2878
N/A	13-Aug-2024	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID: CVE-2024-38148**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38148	O-MIC-WIND-080824/2879
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2880
N/A	13-Aug-2024	7.5	Windows DNS Spoofing Vulnerability **CVE ID: CVE-2024-37968**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37968	O-MIC-WIND-080824/2881
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT)	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2882

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	lity/CVE-2024-38126	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38137**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38137	O-MIC-WIND-080824/2883
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38136**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38136	O-MIC-WIND-080824/2884
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2885
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2886

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	6.5	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability **CVE ID: CVE-2024-38214**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38214	O-MIC-WIND-080824/2887
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2888
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2889
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2890
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143	O-MIC-WIND-080824/2891
Product: windows_server_2022_23h2					
Affected Version(s): * Up to (excluding) 10.0.25398.1009					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38184	O-MIC-WIND-080824/2892
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38185**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38185	O-MIC-WIND-080824/2893
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38186	O-MIC-WIND-080824/2894
N/A	13-Aug-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38187**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38187	O-MIC-WIND-080824/2895
N/A	13-Aug-2024	7.8	Kernel Streaming Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38191**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38191	O-MIC-WIND-080824/2896
Affected Version(s): * Up to (excluding) 10.0.25398.1085					
N/A	13-Aug-2024	9.8	Windows TCP/IP Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2897

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38063	lity/CVE-2024-38063	
N/A	13-Aug-2024	9.8	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38140**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140	O-MIC-WIND-080824/2898
N/A	13-Aug-2024	9.8	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38199**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199	O-MIC-WIND-080824/2899
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38116**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116	O-MIC-WIND-080824/2900
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability **CVE ID: CVE-2024-38114**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114	O-MIC-WIND-080824/2901
N/A	13-Aug-2024	8.8	Windows IP Routing Management Snapin Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115	O-MIC-WIND-080824/2902

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38115		
N/A	13-Aug-2024	8.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38144**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144	O-MIC-WIND-080824/2903
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38120**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38120	O-MIC-WIND-080824/2904
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38121**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38121	O-MIC-WIND-080824/2905
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38128**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38128	O-MIC-WIND-080824/2906
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38130	O-MIC-WIND-080824/2907

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38130		
N/A	13-Aug-2024	8.8	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability **CVE ID: CVE-2024-38131**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38131	O-MIC-WIND-080824/2908
N/A	13-Aug-2024	8.8	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38154	O-MIC-WIND-080824/2909
N/A	13-Aug-2024	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180	O-MIC-WIND-080824/2910
N/A	13-Aug-2024	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38147**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38147	O-MIC-WIND-080824/2911
N/A	13-Aug-2024	7.8	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38107**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107	O-MIC-WIND-080824/2912

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38125**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125	O-MIC-WIND-080824/2913
N/A	13-Aug-2024	7.8	NTFS Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38117**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38117	O-MIC-WIND-080824/2914
N/A	13-Aug-2024	7.8	Windows Secure Kernel Mode Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38142**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38142	O-MIC-WIND-080824/2915
N/A	13-Aug-2024	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38135**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38135	O-MIC-WIND-080824/2916
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38141**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141	O-MIC-WIND-080824/2917
N/A	13-Aug-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38127	O-MIC-WIND-080824/2918

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38127		
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38133**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38133	O-MIC-WIND-080824/2919
Out-of-bounds Read	13-Aug-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38134	O-MIC-WIND-080824/2920
N/A	13-Aug-2024	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38150**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38150	O-MIC-WIND-080824/2921
N/A	13-Aug-2024	7.8	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38193**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193	O-MIC-WIND-080824/2922
N/A	13-Aug-2024	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID: CVE-2024-38152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152	O-MIC-WIND-080824/2923
N/A	13-Aug-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2924

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38153	lity/CVE-2024-38153	
N/A	13-Aug-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196	O-MIC-WIND-080824/2925
N/A	13-Aug-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38215**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38215	O-MIC-WIND-080824/2926
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38132**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38132	O-MIC-WIND-080824/2927
N/A	13-Aug-2024	7.5	Windows Deployment Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-38138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38138	O-MIC-WIND-080824/2928
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38145**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38145	O-MIC-WIND-080824/2929
N/A	13-Aug-2024	7.5	Scripting Engine Memory	https://msrc.microsoft.com/update-	O-MIC-WIND-080824/2930

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Corruption Vulnerability **CVE ID: CVE-2024-38178**	guide/vulnerability/CVE-2024-38178	
N/A	13-Aug-2024	7.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38146**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146	O-MIC-WIND-080824/2931
N/A	13-Aug-2024	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID: CVE-2024-38148**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38148	O-MIC-WIND-080824/2932
N/A	13-Aug-2024	7.5	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38198**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198	O-MIC-WIND-080824/2933
N/A	13-Aug-2024	7.5	Windows DNS Spoofing Vulnerability **CVE ID: CVE-2024-37968**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37968	O-MIC-WIND-080824/2934
N/A	13-Aug-2024	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID: CVE-2024-38126**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38126	O-MIC-WIND-080824/2935
Concurrent Execution using Shared	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-080824/2936

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			Privilege Vulnerability **CVE ID: CVE-2024-38137**	lity/CVE-2024-38137	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-Aug-2024	7	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38136**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38136	O-MIC-WIND-080824/2937
N/A	13-Aug-2024	7	Windows Kernel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38106**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106	O-MIC-WIND-080824/2938
N/A	13-Aug-2024	6.8	Windows Initial Machine Configuration Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38223**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38223	O-MIC-WIND-080824/2939
N/A	13-Aug-2024	6.5	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability **CVE ID: CVE-2024-38214**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38214	O-MIC-WIND-080824/2940

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38122**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122	O-MIC-WIND-080824/2941
Use of Uninitialized Resource	13-Aug-2024	5.5	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability **CVE ID: CVE-2024-38118**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38118	O-MIC-WIND-080824/2942
N/A	13-Aug-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38151	O-MIC-WIND-080824/2943
N/A	13-Aug-2024	4.2	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143	O-MIC-WIND-080824/2944
Affected Version(s): * Up to (excluding) 10.0.25398.950					
N/A	13-Aug-2024	6.5	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38213**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213	O-MIC-WIND-080824/2945
Vendor: nissan-global					
Product: blind_spot_detection_sensor_ecu_firmware					
Affected Version(s): -					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	15-Aug-2024	6.5	* Unprotected privileged mode access through UDS session in the Blind Spot Detection Sensor ECU firmware in Nissan Altima (2022) allows attackers to trigger denial-of-service (DoS) by unauthorized access to the ECU's programming session. * No preconditions implemented for ECU management functionality through UDS session in the Blind Spot Detection Sensor ECU in Nissan Altima (2022) allows attackers to disrupt normal ECU operations by triggering a control command without authentication. **CVE ID: CVE-2024-6347**	N/A	O-NIS-BLIN-080824/2946
Vendor: Paloaltonetworks					
Product: pan-os					
Affected Version(s): From (including) 10.2.0 Up to (excluding) 10.2.8					
Cleartext Storage of Sensitive Information	14-Aug-2024	4.4	An information exposure vulnerability in Palo Alto Networks PAN-OS software	https://security.paloaltonetworks.com/CVE-2024-5916	O-PAL-PAN--080824/2947

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enables a local system administrator to unintentionally disclose secrets, passwords, and tokens of external systems. A read-only administrator who has access to the config log, can read secrets, passwords, and tokens to external systems. **CVE ID: CVE-2024-5916**		
Affected Version(s): From (including) 11.0.0 Up to (excluding) 11.0.4					
Cleartext Storage of Sensitive Information	14-Aug-2024	4.4	An information exposure vulnerability in Palo Alto Networks PAN-OS software enables a local system administrator to unintentionally disclose secrets, passwords, and tokens of external systems. A read-only administrator who has access to the config log, can read secrets, passwords, and tokens to external systems. **CVE ID: CVE-2024-5916**	https://security.paloaltonetworks.com/CVE-2024-5916	O-PAL-PAN--080824/2948
Vendor: raisecom					
Product: msg1200_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 3.90					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90 and classified as critical. Affected by this issue is the function sslvpn_config_mod of the file /vpn/list_ip_network.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273560. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7467**	N/A	O-RAI-MSG1-080824/2949
Improper Neutralization of Special Elements	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and	N/A	O-RAI-MSG1-080824/2950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			MSG2300 3.90. It has been classified as critical. This affects the function sslvpn_config_mod of the file /vpn/list_service_manage.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273561 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7468**		
Improper Neutralization of Special Elements used in an OS Command ('OS	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been declared as critical. This vulnerability affects the function	N/A	O-RAI-MSG1-080824/2951

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			sslvpn_config_mod of the file /vpn/list_vpn_web_custom.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273562 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7469**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been rated as critical. This issue affects the function sslvpn_config_mod of the file /vpn/vpn_template_style.php of the component Web	N/A	O-RAI-MSG1-080824/2952

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273563. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7470**		
Product: msg2100e_firmware					
Affected Version(s): 3.90					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90 and classified as critical. Affected by this issue is the function sslvpn_config_mod of the file /vpn/list_ip_network.php of the component Web Interface. The manipulation of the argument	N/A	O-RAI-MSG2-080824/2953

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			template/stylenum leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273560. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7467**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been classified as critical. This affects the function sslvpn_config_mod of the file /vpn/list_service_manage.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. It is possible to initiate the attack remotely. The	N/A	O-RAI-MSG2-080824/2954

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. The identifier VDB-273561 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7468**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been declared as critical. This vulnerability affects the function sslvpn_config_mod of the file /vpn/list_vpn_web_custom.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273562 is the	N/A	O-RAI-MSG2-080824/2955

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7469**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been rated as critical. This issue affects the function sslvpn_config_mod of the file /vpn/vpn_template_style.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273563. NOTE: The vendor was contacted early	N/A	O-RAI-MSG2-080824/2956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7470**		
Product: msg2200_firmware					
Affected Version(s): 3.90					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90 and classified as critical. Affected by this issue is the function sslvpn_config_mod of the file /vpn/list_ip_network.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273560. NOTE: The vendor was contacted early about this disclosure but did	N/A	O-RAI-MSG2-080824/2957

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID: CVE-2024-7467**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been classified as critical. This affects the function sslvpn_config_mod of the file /vpn/list_service_manage.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273561 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7468**	N/A	O-RAI-MSG2-080824/2958

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been declared as critical. This vulnerability affects the function sslvpn_config_mod of the file /vpn/list_vpn_web_custom.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273562 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7469**	N/A	O-RAI-MSG2-080824/2959
Improper Neutralization of Special	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E,	N/A	O-RAI-MSG2-080824/2960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			MSG2200 and MSG2300 3.90. It has been rated as critical. This issue affects the function sslvpn_config_mod of the file /vpn/vpn_template_style.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273563. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7470**		
Product: msg2300_firmware					
Affected Version(s): 3.90					
Improper Neutralization of Special Elements used in an OS	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90 and classified as critical.	N/A	O-RAI-MSG2-080824/2961

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			Affected by this issue is the function sslvpn_config_mod of the file /vpn/list_ip_network.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273560. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7467**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been classified as critical. This affects the function sslvpn_config_mod of the file /vpn/list_service_manage.php of the	N/A	O-RAI-MSG2-080824/2962

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273561 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7468**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been declared as critical. This vulnerability affects the function sslvpn_config_mod of the file /vpn/list_vpn_web_custom.php of the component Web Interface. The manipulation of the argument	N/A	O-RAI-MSG2-080824/2963

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			template/stylenum leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273562 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7469**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2024	9.8	A vulnerability was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. It has been rated as critical. This issue affects the function sslvpn_config_mod of the file /vpn/vpn_template_style.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The attack may be initiated remotely.	N/A	O-RAI-MSG2-080824/2964

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273563. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7470**		
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 8.0					
NULL Pointer Dereference	12-Aug-2024	7.5	A null pointer dereference flaw was found in Libtiff via `tif_dirinfo.c`. This issue may allow an attacker to trigger memory allocation failures through certain means, such as restricting the heap space size or injecting faults, causing a segmentation fault. This can cause an application crash, eventually leading to a denial of service. **CVE ID: CVE-2024-7006**	N/A	O-RED-ENTE-080824/2965

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.0					
NULL Pointer Dereference	12-Aug-2024	7.5	A null pointer dereference flaw was found in Libtiff via `tif_dirinfo.c`. This issue may allow an attacker to trigger memory allocation failures through certain means, such as restricting the heap space size or injecting faults, causing a segmentation fault. This can cause an application crash, eventually leading to a denial of service. **CVE ID: CVE-2024-7006**	N/A	O-RED-ENTE-080824/2966
Vendor: Samsung					
Product: android					
Affected Version(s): 12.0					
N/A	07-Aug-2024	8.8	Improper input validation in librtp.so prior to SMR Aug-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34619**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2967

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2024	7.8	Out-of-bound write in libcodec2secmp4vdec.so prior to SMR Aug-2024 Release 1 allows local attackers to execute arbitrary code. **CVE ID: CVE-2024-34612**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2968
Out-of-bounds Write	07-Aug-2024	7.8	Out-of-bound write in libsmat.so prior to SMR Aug-2024 Release 1 allows local attackers to execute arbitrary code. **CVE ID: CVE-2024-34614**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2969
Out-of-bounds Write	07-Aug-2024	7.8	Out-of-bound write in libsmat.so prior to SMR Aug-2024 Release 1 allows local attackers to cause memory corruption. **CVE ID: CVE-2024-34615**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2970
N/A	07-Aug-2024	5.5	Improper access control in LedCoverService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background.	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2971

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-34604		
N/A	07-Aug-2024	5.5	Improper access control in SamsungHealthService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34605**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2972
N/A	07-Aug-2024	5.5	Improper access control in SmartThingsService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34606**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2973
N/A	07-Aug-2024	5.5	Improper access control in SamsungNotesService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34607**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2974

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Aug-2024	5.5	Improper access control in PaymentManagerService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34608**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2975
N/A	07-Aug-2024	5.5	Improper access control in VoiceNoteService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34609**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2976
N/A	07-Aug-2024	5.5	Improper access control in ExtControlDeviceService prior to SMR Aug-2024 Release 1 allows local attackers to access protected data. **CVE ID: CVE-2024-34610**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2977
N/A	07-Aug-2024	5.5	Improper access control in KnoxService prior to SMR Aug-2024 Release 1 allows local attackers to	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2978

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			get sensitive information. **CVE ID: CVE-2024-34611**		
Incorrect Default Permissions	07-Aug-2024	5.5	Improper handling of insufficient permission in KnoxDualDARPolicy prior to SMR Aug-2024 Release 1 allows local attackers to access sensitive data. **CVE ID: CVE-2024-34616**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2979
N/A	07-Aug-2024	3.3	Improper access control in System property prior to SMR Aug-2024 Release 1 allows local attackers to access cell related information. **CVE ID: CVE-2024-34618**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2980
Affected Version(s): 14.0					
N/A	07-Aug-2024	8.8	Improper input validation in librtp.so prior to SMR Aug-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34619**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2981

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2024	7.8	Out-of-bound write in libcodec2secmp4vdec.so prior to SMR Aug-2024 Release 1 allows local attackers to execute arbitrary code. **CVE ID: CVE-2024-34612**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2982
Out-of-bounds Write	07-Aug-2024	7.8	Out-of-bound write in libsmat.so prior to SMR Aug-2024 Release 1 allows local attackers to execute arbitrary code. **CVE ID: CVE-2024-34614**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2983
Out-of-bounds Write	07-Aug-2024	7.8	Out-of-bound write in libsmat.so prior to SMR Aug-2024 Release 1 allows local attackers to cause memory corruption. **CVE ID: CVE-2024-34615**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2984
N/A	07-Aug-2024	7.8	Improper privilege management in SumeNNService prior to SMR Aug-2024 Release 1 allows local attackers to start privileged service. **CVE ID: CVE-2024-34620**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2985
N/A	07-Aug-2024	5.5	Improper access control in	https://security.samsungmobile	O-SAM-ANDR-080824/2986

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LedCoverService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34604**	.com/securityUpdate.smsb?year=2024&month=08	
N/A	07-Aug-2024	5.5	Improper access control in SamsungHealthService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34605**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2987
N/A	07-Aug-2024	5.5	Improper access control in SmartThingsService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34606**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2988
N/A	07-Aug-2024	5.5	Improper access control in SamsungNotesService prior to SMR Aug-2024 Release 1	https://security.samsungmobile.com/securityUpdate.smsb?yea	O-SAM-ANDR-080824/2989

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34607**	r=2024&month=08	
N/A	07-Aug-2024	5.5	Improper access control in PaymentManagerService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34608**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2990
N/A	07-Aug-2024	5.5	Improper access control in VoiceNoteService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34609**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2991
N/A	07-Aug-2024	5.5	Improper access control in ExtControlDeviceService prior to SMR Aug-2024 Release 1 allows local attackers to access protected data.	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2992

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-34610		
N/A	07-Aug-2024	5.5	Improper access control in KnoxService prior to SMR Aug-2024 Release 1 allows local attackers to get sensitive information. **CVE ID: CVE-2024-34611**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2993
Incorrect Default Permissions	07-Aug-2024	5.5	Improper handling of insufficient permission in KnoxDualDARPolicy prior to SMR Aug-2024 Release 1 allows local attackers to access sensitive data. **CVE ID: CVE-2024-34616**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2994
Incorrect Default Permissions	07-Aug-2024	3.3	Improper handling of insufficient permission in Telephony prior to SMR Aug-2024 Release 1 allows local attackers to configure default Message application. **CVE ID: CVE-2024-34617**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2995
N/A	07-Aug-2024	3.3	Improper access control in System property prior to SMR Aug-2024 Release 1 allows local attackers to	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2996

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access cell related information. **CVE ID: CVE-2024-34618**		
Affected Version(s): 13.0					
N/A	07-Aug-2024	8.8	Improper input validation in librtp.so prior to SMR Aug-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34619**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2997
Out-of-bounds Write	07-Aug-2024	7.8	Out-of-bound write in libcodec2secmp4vdec.so prior to SMR Aug-2024 Release 1 allows local attackers to execute arbitrary code. **CVE ID: CVE-2024-34612**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2998
Out-of-bounds Write	07-Aug-2024	7.8	Out-of-bound write in libsmat.so prior to SMR Aug-2024 Release 1 allows local attackers to execute arbitrary code. **CVE ID: CVE-2024-34614**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/2999

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2024	7.8	Out-of-bound write in libsmat.so prior to SMR Aug-2024 Release 1 allows local attackers to cause memory corruption. **CVE ID: CVE-2024-34615**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/3000
N/A	07-Aug-2024	7.8	Improper privilege management in SumeNNService prior to SMR Aug-2024 Release 1 allows local attackers to start privileged service. **CVE ID: CVE-2024-34620**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/3001
N/A	07-Aug-2024	5.5	Improper access control in LedCoverService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34604**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/3002
N/A	07-Aug-2024	5.5	Improper access control in SamsungHealthService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/3003

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from the background. **CVE ID: CVE-2024-34605**		
N/A	07-Aug-2024	5.5	Improper access control in SmartThingsService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34606**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/3004
N/A	07-Aug-2024	5.5	Improper access control in SamsungNotesService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34607**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/3005
N/A	07-Aug-2024	5.5	Improper access control in PaymentManagerService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background.	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/3006

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-34608		
N/A	07-Aug-2024	5.5	Improper access control in VoiceNoteService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34609**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/3007
N/A	07-Aug-2024	5.5	Improper access control in ExtControlDeviceService prior to SMR Aug-2024 Release 1 allows local attackers to access protected data. **CVE ID: CVE-2024-34610**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/3008
N/A	07-Aug-2024	5.5	Improper access control in KnoxService prior to SMR Aug-2024 Release 1 allows local attackers to get sensitive information. **CVE ID: CVE-2024-34611**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/3009
Incorrect Default Permissions	07-Aug-2024	5.5	Improper handling of insufficient permission in KnoxDualDARPolicy prior to SMR Aug-2024 Release 1 allows local	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/3010

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to access sensitive data. **CVE ID: CVE-2024-34616**		
N/A	07-Aug-2024	3.3	Improper access control in System property prior to SMR Aug-2024 Release 1 allows local attackers to access cell related information. **CVE ID: CVE-2024-34618**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-080824/3011
Product: wear_os					
Affected Version(s): 4.0					
N/A	07-Aug-2024	5.5	Improper access control in Galaxy Watch prior to SMR Aug-2024 Release 1 allows local attackers to access sensitive information of Galaxy watch. **CVE ID: CVE-2024-34613**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-WEAR-080824/3012
Vendor: Sprecher-automation					
Product: sprecon-e-c_firmware					
Affected Version(s): * Up to (excluding) 8.71j					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	O-SPR-SPRE-080824/3013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protection assignments. **CVE ID: CVE-2024-6758**		
Product: sprecon-e-p_dd6-2_firmware					
Affected Version(s): * Up to (excluding) 8.71j					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	O-SPR-SPRE-080824/3014
Product: sprecon-e-p_dl6-1_firmware					
Affected Version(s): * Up to (excluding) 8.71j					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	O-SPR-SPRE-080824/3015
Product: sprecon-e-p_dq6-1_firmware					
Affected Version(s): * Up to (excluding) 8.71j					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below	https://www.sprecher-automation.com/fileadmin/itSe	O-SPR-SPRE-080824/3016

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	curity/PDF/SPR-2407171_de.pdf	
Product: sprecon-e-p_ds6-0_firmware					
Affected Version(s): * Up to (excluding) 8.71j					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	O-SPR-SPRE-080824/3017
Product: sprecon-e-t3_ax-3110_firmware					
Affected Version(s): * Up to (excluding) 8.71j					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	O-SPR-SPRE-080824/3018
Product: sprecon-e-t3_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 8.71j					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	O-SPR-SPRE-080824/3019
Product: sprecon-edir_firmware					
Affected Version(s): * Up to (excluding) 8.71j					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	O-SPR-SPRE-080824/3020
Product: sprecon-e_ap-2200_firmware					
Affected Version(s): * Up to (excluding) 8.71j					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	O-SPR-SPRE-080824/3021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protection assignments. **CVE ID: CVE-2024-6758**		
Product: sprecon-e_cp-2131_firmware					
Affected Version(s): * Up to (excluding) 8.71j					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	O-SPR-SPRE-080824/3022
Product: sprecon-e_cp-2330_firmware					
Affected Version(s): * Up to (excluding) 8.71j					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	https://www.sprecher-automation.com/fileadmin/itSecurity/PDF/SPR-2407171_de.pdf	O-SPR-SPRE-080824/3023
Product: sprecon-e_cp-2500_firmware					
Affected Version(s): * Up to (excluding) 8.71j					
N/A	12-Aug-2024	6.5	Improper Privilege Management in Sprecher Automation SPRECON-E below	https://www.sprecher-automation.com/fileadmin/itSe	O-SPR-SPRE-080824/3024

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments. **CVE ID: CVE-2024-6758**	curity/PDF/SPR-2407171_de.pdf	
Vendor: Tenda					
Product: fh1201_firmware					
Affected Version(s): 1.2.0.14\\(408\\)					
N/A	15-Aug-2024	9.8	An issue in the handler function in /goform/telnet of Tenda FH1201 v1.2.0.14 (408) allows attackers to execute arbitrary commands via a crafted HTTP request. **CVE ID: CVE-2024-42947**	N/A	O-TEN-FH12-080824/3025
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromP2pListFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42940**	N/A	O-TEN-FH12-080824/3026

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the wanmode parameter in the fromAdvSetWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42941**	N/A	O-TEN-FH12-080824/3027
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the PPPOEPassword parameter in the fromAdvSetWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42943**	N/A	O-TEN-FH12-080824/3028
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromNatlimit function. This vulnerability	N/A	O-TEN-FH12-080824/3029

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42944**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromVirtualSer function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42946**	N/A	O-TEN-FH12-080824/3030
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the delno parameter in the fromPptpUserSetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42948**	N/A	O-TEN-FH12-080824/3031

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the Go parameter in the fromSafeClientFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42950**	N/A	O-TEN-FH12-080824/3032
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the mit_pptpusrpw parameter in the fromWizardHandle function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42951**	N/A	O-TEN-FH12-080824/3033
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromqossetting function. This vulnerability allows attackers to	N/A	O-TEN-FH12-080824/3034

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42952**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromSafeClientFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42955**	N/A	O-TEN-FH12-080824/3035
Product: fh1206_firmware					
Affected Version(s): 02.03.01.35					
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the Go parameter in the fromSafeUrlFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42968**	N/A	O-TEN-FH12-080824/3036

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromSetIpBind function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42973**	N/A	O-TEN-FH12-080824/3037
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromwebExcptypemanFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42974**	N/A	O-TEN-FH12-080824/3038
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the frmL7ProtForm function. This vulnerability allows attackers to	N/A	O-TEN-FH12-080824/3039

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42979**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the pptpPPW parameter in the fromAdvSetWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42983**	N/A	O-TEN-FH12-080824/3040
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromP2pListFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42984**	N/A	O-TEN-FH12-080824/3041
Affected Version(s): 1.2.0.8\\(8155\\)					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Aug-2024	9.8	A vulnerability was found in Tenda FH1206 1.2.0.8(8155) and classified as critical. This issue affects the function fromGstDhcpSetSer of the file /goform/GstDhcpSetSer. The manipulation of the argument dips leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7613**	N/A	O-TEN-FH12-080824/3042
Out-of-bounds Write	12-Aug-2024	9.8	A vulnerability was found in Tenda FH1206 1.2.0.8(8155). It has been classified as critical. Affected is the function fromqossetting of the file /goform/qossetting. The manipulation of the argument page leads to stack-based buffer	N/A	O-TEN-FH12-080824/3043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7614**		
Out-of-bounds Write	12-Aug-2024	9.8	A vulnerability was found in Tenda FH1206 1.2.0.8. It has been declared as critical. Affected by this vulnerability is the function fromSafeClientFilter/fromSafeMacFilter/fromSafeUrlFilter. The manipulation leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	O-TEN-FH12-080824/3044

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7615		
Affected Version(s): v02.03.01.35					
N/A	15-Aug-2024	9.8	An issue in the handler function in /goform/telnet of Tenda FH1206 v02.03.01.35 allows attackers to execute arbitrary commands via a crafted HTTP request. **CVE ID: CVE-2024-42978**	N/A	O-TEN-FH12-080824/3045
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromSafeUrlFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42969**	N/A	O-TEN-FH12-080824/3046
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromSafeClientFilter function. This vulnerability	N/A	O-TEN-FH12-080824/3047

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42976**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the qos parameter in the fromqossetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42977**	N/A	O-TEN-FH12-080824/3048
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the frmL7ImForm function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42980**	N/A	O-TEN-FH12-080824/3049
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to	N/A	O-TEN-FH12-080824/3050

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow via the delno parameter in the fromPptpUserSetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42981**		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromVirtualSer function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42982**	N/A	O-TEN-FH12-080824/3051
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromNatlimit function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a	N/A	O-TEN-FH12-080824/3052

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted POST request. **CVE ID: CVE-2024-42985**		
Affected Version(s): v02.03.1.35					
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the PPPOEPassword parameter in the fromAdvSetWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42986**	N/A	O-TEN-FH12-080824/3053
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the modino parameter in the fromPptpUserAdd function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42987**	N/A	O-TEN-FH12-080824/3054
Product: i22_firmware					
Affected Version(s): 1.0.0.3\\(4687\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2024	9.8	A vulnerability classified as critical was found in Tenda i22 1.0.0.3(4687). This vulnerability affects the function formApPortalAccessCodeAuth of the file /goform/apPortalAccessCodeAuth. The manipulation of the argument accessCode/data/acceInfo leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7582**	N/A	O-TEN-I22_-080824/3055
Out-of-bounds Write	07-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda i22 1.0.0.3(4687). This issue affects the function formApPortalOneKeyAuth of the file /goform/apPortalOneKeyAuth. The manipulation of the	N/A	O-TEN-I22_-080824/3056

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument data leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7583**		
Vendor: Tendacn					
Product: a301_firmware					
Affected Version(s): 15.13.08.12					
Out-of-bounds Write	07-Aug-2024	9.8	A vulnerability classified as critical has been found in Tenda A301 15.13.08.12. This affects the function formWifiBasicSet of the file /goform/WifiBasicSet. The manipulation of the argument security leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The	N/A	O-TEN-A301-080824/3057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7581**		
Product: fh1201_firmware					
Affected Version(s): 1.2.0.14\\(408\\)					
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the frmL7ImForm function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42942**	N/A	O-TEN-FH12-080824/3058
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromAddressNat function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	N/A	O-TEN-FH12-080824/3059

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42945		
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the qos parameter in the fromqossetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42949**	N/A	O-TEN-FH12-080824/3060
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the PPW parameter in the fromWizardHandle function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42953**	N/A	O-TEN-FH12-080824/3061
Out-of-bounds Write	15-Aug-2024	7.5	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the	N/A	O-TEN-FH12-080824/3062

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fromwebExcptype manFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID: CVE-2024-42954**		
Vendor: totolink					
Product: a3002r_firmware					
Affected Version(s): 4.0.0-b20230531.1404					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Aug-2024	9.8	TOTOLINK A3002R v4.0.0-B20230531.1404 contains a buffer overflow vulnerability in /bin/boa via formParentControl. **CVE ID: CVE-2024-42520**	N/A	O-TOT-A300-080824/3063
Product: a3100r_firmware					
Affected Version(s): 4.1.2cu.5050_b20200504					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Aug-2024	9.8	TOTOLINK A3100R V4.1.2cu.5050_B20200504 has a buffer overflow vulnerability in the password parameter in the loginauth function. **CVE ID: CVE-2024-42546**	N/A	O-TOT-A310-080824/3064
Buffer Copy without Checking Size of	12-Aug-2024	9.8	TOTOLINK A3100R V4.1.2cu.5050_B20200504 has a buffer overflow vulnerability in the	N/A	O-TOT-A310-080824/3065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			http_host parameter in the loginauth function. **CVE ID: CVE-2024-42547**		
Product: a3700r_firmware					
Affected Version(s): 9.1.2u.5822_b20200513					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Aug-2024	9.8	TOTOLINK A3700R v9.1.2u.5822_B20200513 has a buffer overflow vulnerability in the http_host parameter in the loginauth function. **CVE ID: CVE-2024-42543**	N/A	O-TOT-A370-080824/3066
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Aug-2024	9.8	TOTOLINK A3700R v9.1.2u.5822_B20200513 has a buffer overflow vulnerability in the ssid parameter in setWizardCfg function. **CVE ID: CVE-2024-42545**	N/A	O-TOT-A370-080824/3067
Product: cp450_firmware					
Affected Version(s): 4.1.0cu.747_b20191224					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in TOTOLINK CP450 4.1.0cu.747_B20191224. Affected is the function loginauth of the file /cgi-bin/cstecgi.cgi. The	N/A	O-TOT-CP45-080824/3068

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument http_host leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-273558 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7465**		
Product: cp900_firmware					
Affected Version(s): 6.3c.566					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2024	9.8	A vulnerability classified as critical was found in TOTOLINK CP900 6.3c.566. This vulnerability affects the function UploadCustomModule of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument File leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The	N/A	O-TOT-CP90-080824/3069

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier of this vulnerability is VDB-273556. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7463**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in TOTOLINK CP900 6.3c.566. This issue affects the function setTelnetCfg of the component Telnet Service. The manipulation of the argument telnet_enabled leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273557 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	O-TOT-CP90-080824/3070

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7464		
Product: lr350_firmware					
Affected Version(s): 9.3.5u.6369_b20220309					
N/A	15-Aug-2024	9.8	Incorrect access control in TOTOLINK LR350 V9.3.5u.6369_B20220309 allows attackers to obtain the apmib configuration file, which contains the username and the password, via a crafted request to /cgi-bin/ExportSettings.sh. **CVE ID: CVE-2024-42967**	N/A	O-TOT-LR35-080824/3071
Product: n350rt_firmware					
Affected Version(s): 9.3.5u.6139_b20201216					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2024	9.8	A vulnerability classified as critical has been found in TOTOLINK N350RT 9.3.5u.6139_B20201216. This affects the function setWizardCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ssid leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the	N/A	O-TOT-N350-080824/3072

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. The associated identifier of this vulnerability is VDB-273555. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7462**		
N/A	15-Aug-2024	9.8	Incorrect access control in TOTOLINK N350RT V9.3.5u.6139_B20201216 allows attackers to obtain the apmib configuration file, which contains the username and the password, via a crafted request to /cgi-bin/ExportSettings.sh. **CVE ID: CVE-2024-42966**	N/A	O-TOT-N350-080824/3073
Product: x5000r_firmware					
Affected Version(s): 9.1.0u.6369_b20230113					
Improper Neutralization of Special Elements used in an OS Command ('OS	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setL2tpServerCfg.	N/A	O-TOT-X500-080824/3074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42741**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setUrlFilterRules. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42742**	N/A	O-TOT-X500-080824/3075
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setSyslogCfg . Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42743**	N/A	O-TOT-X500-080824/3076
Improper Neutralization of	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20	N/A	O-TOT-X500-080824/3077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setModifyVpnUser. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42744**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setUPnPCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42745**	N/A	O-TOT-X500-080824/3078
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setWanIeCfg. Authenticated Attackers can send malicious packet to	N/A	O-TOT-X500-080824/3079

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands. **CVE ID: CVE-2024-42747**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setWiFiWpsCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42748**	N/A	O-TOT-X500-080824/3080
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	13-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in delBlacklist. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42737**	N/A	O-TOT-X500-080824/3081
Improper Neutralization of Special Elements used in an	13-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS	N/A	O-TOT-X500-080824/3082

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			command injection vulnerability in setDmzCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42738**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	13-Aug-2024	8.8	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setAccessDeviceCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands. **CVE ID: CVE-2024-42739**	N/A	O-TOT-X500-080824/3083
Vendor: Vivotek					
Product: cc8160_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Vivotek CC8160 VVTK-0100d and classified as critical. Affected by this issue is the function read of the component httpd. The manipulation of the argument	N/A	O-VIV-CC81-080824/3084

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Content-Length leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273524. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the affected release tree is end-of-life. **CVE ID: CVE-2024-7439**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Vivotek CC8160 VVTK-0100d. It has been classified as critical. This affects the function getenv of the file upload_file.cgi. The manipulation of the argument QUERY_STRING leads to command injection. It is possible to initiate	N/A	O-VIV-CC81-080824/3085

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attack remotely. The identifier VDB-273525 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the affected release tree is end-of-life. **CVE ID: CVE-2024-7440**		
Product: ib8367a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical has been found in Vivotek IB8367A VVTK-0100b. Affected is the function getenv of the file upload_file.cgi. The manipulation of the argument QUERY_STRING leads to command injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-273528.	N/A	O-VIV-IB83-080824/3086

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the affected release tree is end-of-life. **CVE ID: CVE-2024-7443**		
Product: sd9364_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Vivotek SD9364 VVTK-0103f. It has been declared as critical. This vulnerability affects the function read of the component httpd. The manipulation of the argument Content-Length leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273526 is the identifier assigned to this vulnerability.	N/A	O-VIV-SD93-080824/3087

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the affected release tree is end-of-life. **CVE ID: CVE-2024-7441**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Aug-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Vivotek SD9364 VVTK-0103f. It has been rated as critical. This issue affects the function getenv of the file upload_file.cgi. The manipulation of the argument QUERY_STRING leads to command injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-273527. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and	N/A	O-VIV-SD93-080824/3088

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confirmed that the affected release tree is end-of-life. **CVE ID: CVE-2024-7442**		
Vendor: vonets					
Product: vap11ac_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	O-VON-VAP1-080824/3089
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to	N/A	O-VON-VAP1-080824/3090

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	O-VON-VAP1-080824/3091
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets	N/A	O-VON-VAP1-080824/3092

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via	N/A	O-VON-VAP1-080824/3093

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	O-VON-VAP1-080824/3094
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9	N/A	O-VON-VAP1-080824/3095

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**		
Product: vap11g-300_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	O-VON-VAP1-080824/3096
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an	N/A	O-VON-VAP1-080824/3097

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	O-VON-VAP1-080824/3098
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets	N/A	O-VON-VAP1-080824/3099

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass	N/A	O-VON-VAP1-080824/3100

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	O-VON-VAP1-080824/3101
Improper Limitation of a Pathname to a Restricted	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and	N/A	O-VON-VAP1-080824/3102

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**		
Product: vap11g-500s_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	O-VON-VAP1-080824/3103
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge	N/A	O-VON-VAP1-080824/3104

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	O-VON-VAP1-080824/3105
Direct Request	12-Aug-2024	9.8	An improper authentication	N/A	O-VON-VAP1-080824/3106

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Forced Browsing')			vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated	N/A	O-VON-VAP1-080824/3107

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	O-VON-VAP1-080824/3108
Improper Limitation of a Pathname	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets	N/A	O-VON-VAP1-080824/3109

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**		
Product: vap11g-500_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	O-VON-VAP1-080824/3110
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and	N/A	O-VON-VAP1-080824/3111

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	O-VON-VAP1-080824/3112

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**	N/A	O-VON-VAP1-080824/3113
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9	N/A	O-VON-VAP1-080824/3114

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	O-VON-VAP1-080824/3115

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	O-VON-VAP1-080824/3116
Product: vap11g_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	O-VON-VAP1-080824/3117
Use of Hard-	08-Aug-2024	9.8	Use of hard-coded credentials	N/A	O-VON-VAP1-080824/3118

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to	N/A	O-VON-VAP1-080824/3119

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code. **CVE ID: CVE-2024-39791**		
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**	N/A	O-VON-VAP1-080824/3120
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets	N/A	O-VON-VAP1-080824/3121

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication	N/A	O-VON-VAP1-080824/3122

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	O-VON-VAP1-080824/3123
Product: vap11n-300_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters.	N/A	O-VON-VAP1-080824/3124

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-37023		
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**	N/A	O-VON-VAP1-080824/3125
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an	N/A	O-VON-VAP1-080824/3126

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**		
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**	N/A	O-VON-VAP1-080824/3127
Improper Access Control	12-Aug-2024	8.6	Improper access control	N/A	O-VON-VAP1-080824/3128

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of	N/A	O-VON-VAP1-080824/3129

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	O-VON-VAP1-080824/3130
Product: vap11s-5g_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker	N/A	O-VON-VAP1-080824/3131

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**		
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**	N/A	O-VON-VAP1-080824/3132
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge	N/A	O-VON-VAP1-080824/3133

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**		
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session.	N/A	O-VON-VAP1-080824/3134

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42001		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	O-VON-VAP1-080824/3135
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9	N/A	O-VON-VAP1-080824/3136

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	O-VON-VAP1-080824/3137
Product: vap11s_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements used in a Command ('Comman	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software	N/A	O-VON-VAP1-080824/3138

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**		
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**	N/A	O-VON-VAP1-080824/3139
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets	N/A	O-VON-VAP1-080824/3140

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**		
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when	N/A	O-VON-VAP1-080824/3141

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	O-VON-VAP1-080824/3142
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software	N/A	O-VON-VAP1-080824/3143

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	O-VON-VAP1-080824/3144
Product: var11n-300_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements used in a Command ('Comman	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and	N/A	O-VON-VAR1-080824/3145

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**		
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**	N/A	O-VON-VAR1-080824/3146
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets	N/A	O-VON-VAR1-080824/3147

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**		
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a	N/A	O-VON-VAR1-080824/3148

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	O-VON-VAR1-080824/3149
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets	N/A	O-VON-VAR1-080824/3150

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	O-VON-VAR1-080824/3151
Product: var1200-h_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets	N/A	O-VON-VAR1-080824/3152

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**		
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**	N/A	O-VON-VAR1-080824/3153
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow	N/A	O-VON-VAR1-080824/3154

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**		
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an	N/A	O-VON-VAR1-080824/3155

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	O-VON-VAR1-080824/3156
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets	N/A	O-VON-VAR1-080824/3157

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	O-VON-VAR1-080824/3158
Product: var1200-l_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	O-VON-VAR1-080824/3159
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled.	N/A	O-VON-VAR1-080824/3160

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41161		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	O-VON-VAR1-080824/3161
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge	N/A	O-VON-VAR1-080824/3162

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	O-VON-VAR1-080824/3163
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional	N/A	O-VON-VAR1-080824/3164

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**	N/A	O-VON-VAR1-080824/3165

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: var600-h_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	O-VON-VAR6-080824/3166
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These	N/A	O-VON-VAR6-080824/3167

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	O-VON-VAR6-080824/3168
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets	N/A	O-VON-VAR6-080824/3169

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints. **CVE ID: CVE-2024-29082**	N/A	O-VON-VAR6-080824/3170

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	O-VON-VAR6-080824/3171
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary	N/A	O-VON-VAR6-080824/3172

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files and bypass authentication. **CVE ID: CVE-2024-41936**		
Product: vbg1200_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	O-VON-VBG1-080824/3173
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication	N/A	O-VON-VBG1-080824/3174

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	O-VON-VBG1-080824/3175
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets	N/A	O-VON-VBG1-080824/3176

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints.	N/A	O-VON-VBG1-080824/3177

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-29082		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	O-VON-VBG1-080824/3178
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated	N/A	O-VON-VBG1-080824/3179

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**		
Product: vga-1000_firmware					
Affected Version(s): * Up to (including) 3.3.23.6.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Aug-2024	9.9	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters. **CVE ID: CVE-2024-37023**	N/A	O-VON-VGA--080824/3180
Use of Hard-coded Credentials	08-Aug-2024	9.8	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and WiFi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to	N/A	O-VON-VGA--080824/3181

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled. **CVE ID: CVE-2024-41161**		
Out-of-bounds Write	12-Aug-2024	9.8	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code. **CVE ID: CVE-2024-39791**	N/A	O-VON-VGA--080824/3182
Direct Request ('Forced Browsing')	12-Aug-2024	9.8	An improper authentication vulnerability affecting Vonets	N/A	O-VON-VGA--080824/3183

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session. **CVE ID: CVE-2024-42001**		
Improper Access Control	12-Aug-2024	8.6	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via	N/A	O-VON-VGA--080824/3184

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unprotected goform endpoints. **CVE ID: CVE-2024-29082**		
N/A	12-Aug-2024	7.5	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service. **CVE ID: CVE-2024-39815**	N/A	O-VON-VGA--080824/3185
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Aug-2024	7.5	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9	N/A	O-VON-VGA--080824/3186

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication. **CVE ID: CVE-2024-41936**		
Vendor: ZTE					
Product: zxv10_et301_firmware					
Affected Version(s): * Up to (excluding) v3.22.11p3					
N/A	08-Aug-2024	8.8	There is a permission and access control vulnerability of ZTE's ZXV10 XT802/ET301 product.Attackers with common permissions can log in the terminal web and change the password of the administrator illegally by intercepting requests to change the passwords. **CVE ID: CVE-2024-22069**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1036424	O-ZTE-ZXV1-080824/3187
Product: zxv10_xt802_firmware					
Affected Version(s): * Up to (excluding) v2.24.10p1					
N/A	08-Aug-2024	8.8	There is a permission and access control vulnerability of ZTE's ZXV10 XT802/ET301 product. Attackers with common	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1036424	O-ZTE-ZXV1-080824/3188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions can log in the terminal web and change the password of the administrator illegally by intercepting requests to change the passwords. **CVE ID: CVE-2024-22069**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

*stands for all versions