National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 – 31 Mar 2024 Vol. 11 No. 06

Table of Content

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: deltaww					
Product: diaenergie					
Affected Version(s): * Up to (excluding) 1.10.00.005					
N/A	21-Mar-2024	8.8	Privileges are not fully verified server-side, which can be abused by a user with limited privileges to bypass authorization and access privileged functionality. **CVE ID : CVE-2024-28029**	N/A	A-DEL-DIAE-040424/1
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 123.0.6312.58					
N/A	20-Mar-2024	8.8	Object lifecycle issue in V8 in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-2625**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-040424/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	20-Mar-2024	8.8	Use after free in Canvas in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2627**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-040424/3
Out-of-bounds Read	20-Mar-2024	6.5	Out of bounds read in Swiftshader in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2626**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-040424/4
N/A	20-Mar-2024	6.5	Inappropriate implementation in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to leak cross-origin data	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-040424/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2630**		
N/A	20-Mar-2024	4.3	Inappropriate implementation in Downloads in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted URL. (Chromium security severity: Medium) **CVE ID : CVE-2024-2628**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-040424/6
N/A	20-Mar-2024	4.3	Incorrect security UI in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2629**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-040424/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Mar-2024	4.3	Inappropriate implementation in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2024-2631**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-040424/8
Vendor: IBM					
Product: cics_transaction_gateway					
Affected Version(s): 9.2					
Insufficiently Protected Credentials	31-Mar-2024	4.9	IBM CICS Transaction Gateway for Multiplatforms 9.2 and 9.3 transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. IBM X-Force ID: 273612. **CVE ID : CVE-2023-50311**	https://https//www.ibm.com/support/pages/node/7145418	A-IBM-CICS-040424/9
Affected Version(s): 9.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	31-Mar-2024	4.9	IBM CICS Transaction Gateway for Multiplatforms 9.2 and 9.3 transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. IBM X-Force ID: 273612. **CVE ID : CVE-2023-50311**	https://https//www.ibm.com/support/pages/node/7145418	A-IBM-CICS-040424/10
Product: cloud_pak_for_business_automation					
Affected Version(s): 18.0.0					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account.	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**		
Affected Version(s): 18.0.1					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/12
Affected Version(s): 18.0.2					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,2	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**		
Affected Version(s): 19.0.1					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938.	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50959		
Affected Version(s): 19.0.2					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/15
Affected Version(s): 19.0.3					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**		
Affected Version(s): 20.0.1					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/17
Affected Version(s): 20.0.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/18
Affected Version(s): 20.0.3					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**		
Affected Version(s): 21.0.1					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/20
Affected Version(s): 21.0.2					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1,	https://exchange.xforce.ibmcloud.com/vulnerabilities/2759	A-IBM-CLOU-040424/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**	38, https://www.ibm.com/support/pages/node/7145492	
Affected Version(s): 21.0.3					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**		
Affected Version(s): 22.0.1					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/23
Affected Version(s): 22.0.2					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3,	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support	A-IBM-CLOU-040424/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**	/pages/node/7145492	
Affected Version(s): 23.0.1					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938.	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/25

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50959		
Affected Version(s): 23.0.2					
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,22.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938. **CVE ID : CVE-2023-50959**	https://exchange.xforce.ibmcloud.com/vulnerabilities/275938, https://www.ibm.com/support/pages/node/7145492	A-IBM-CLOU-040424/26
Product: infosphere_information_server					
Affected Version(s): 11.7					
Insertion of Sensitive Information into Log File	21-Mar-2024	5.5	IBM InfoSphere Information Server 11.7 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 280361.	https://exchange.xforce.ibmcloud.com/vulnerabilities/280361, https://www.ibm.com/support/pages/node/7117184	A-IBM-INFO-040424/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22352		
Product: security_verify_access					
Affected Version(s): 10.0.6					
Missing Encryption of Sensitive Data	31-Mar-2024	5.5	IBM Security Verify Access 10.0.6 could disclose sensitive snapshot information due to missing encryption. IBM X-Force ID: 281607. **CVE ID : CVE-2024-25027**	https://exchange.xforce.ibmcloud.com/vulnerabilities/281607, https://www.ibm.com/support/pages/node/7145400	A-IBM-SECU-040424/28
Product: security_verify_directory					
Affected Version(s): 10.0.0					
Inadequate Encryption Strength	22-Mar-2024	6.5	IBM Security Verify Directory 10.0.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 228444. **CVE ID : CVE-2022-32753**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228444, https://www.ibm.com/support/pages/node/7145001	A-IBM-SECU-040424/29
N/A	22-Mar-2024	5.3	IBM Security Verify Directory 10.0.0 could disclose sensitive server information that could be used in	https://exchange.xforce.ibmcloud.com/vulnerabilities/228437, https://www.ibm.com/support	A-IBM-SECU-040424/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			further attacks against the system. IBM X-Force ID: 228437. **CVE ID : CVE-2022-32751**	/pages/node/7145001	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2024	4.8	IBM Security Verify Directory 10.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 228445. **CVE ID : CVE-2022-32754**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228445, https://www.ibm.com/support/pages/node/7145001	A-IBM-SECU-040424/31
Generation of Error Message Containing Sensitive Information	22-Mar-2024	2.7	IBM Security Verify Directory 10.0.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the	https://exchange.xforce.ibmcloud.com/vulnerabilities/228507, https://www.ibm.com/support/pages/node/7145001	A-IBM-SECU-040424/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. IBM X-Force ID: 228507. **CVE ID : CVE-2022-32756**		
Product: storage_protect_plus					
Affected Version(s): From (including) 10.1.0 Up to (including) 10.1.16					
Improper Privilege Management	21-Mar-2024	4.3	IBM Storage Protect Plus Server 10.1.0 through 10.1.16 could allow an authenticated user with read-only permissions to add or delete entries from an existing HyperVisor configuration. IBM X-Force ID: 271538. **CVE ID : CVE-2023-47715**	https://exchange.xforce.ibmcloud.com/vulnerabilities/271538, https://www.ibm.com/support/pages/node/7144861	A-IBM-STOR-040424/33
Product: websphere_application_server					
Affected Version(s): From (including) 17.0.0.3 Up to (including) 24.0.0.3					
Uncontrolled Resource Consumption	31-Mar-2024	7.5	IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.3 is vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory	https://exchange.xforce.ibmcloud.com/vulnerabilities/280400, https://www.ibm.com/support/pages/node/7145365	A-IBM-WEBS-040424/34

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resources. IBM X-Force ID: 280400. **CVE ID : CVE-2024-22353**		
Vendor: ivanti					
Product: neurons_for_itsm					
Affected Version(s): * Up to (excluding) 2023.4					
Unrestricted Upload of File with Dangerous Type	31-Mar-2024	9.9	An file upload vulnerability in Ivanti ITSM before 2023.4, allows an authenticated remote user to perform file writes to the server. Successful exploitation may lead to execution of commands in the context of non-root user. **CVE ID : CVE-2023-46808**	https://forums.ivanti.com/s/article/SA-CVE-2023-46808-Authenticated-Remote-File-Write-for-Ivanti-Neurons-for-ITSM	A-IVA-NEUR-040424/35
Product: standalone_sentry					
Affected Version(s): * Up to (excluding) 9.19.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	31-Mar-2024	8.8	A command injection vulnerability in Ivanti Sentry prior to 9.19.0 allows unauthenticated threat actor to execute arbitrary commands on the underlying operating system of the appliance within the same physical or logical network.	https://forums.ivanti.com/s/article/CVE-2023-41724-Remote-Code-Execution-for-Ivanti-Standalone-Sentry	A-IVA-STAN-040424/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-41724		
Vendor: Microsoft					
Product: edge					
Affected Version(s): * Up to (excluding) 122.0.2365.63					
N/A	21-Mar-2024	4.3	Microsoft Edge for Android (Chromium-based) Information Disclosure Vulnerability **CVE ID : CVE-2024-26196**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26196	A-MIC-EDGE-040424/37
Affected Version(s): * Up to (excluding) 123.0.2420.53					
N/A	22-Mar-2024	4.7	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability **CVE ID : CVE-2024-26247**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26247	A-MIC-EDGE-040424/38
N/A	22-Mar-2024	4.3	Microsoft Edge (Chromium-based) Spoofing Vulnerability **CVE ID : CVE-2024-29057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29057	A-MIC-EDGE-040424/39
Vendor: Splunk					
Product: splunk					
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.0.9					
Improper Neutralization of Special Elements used in a Command ('Comman	27-Mar-2024	8.1	In Splunk Enterprise versions below 9.2.1, 9.1.4, and 9.0.9, the Dashboard Examples Hub in the Splunk	https://advisory.splunk.com/advisories/SVD-2024-0302, https://research.splunk.com/application/1cf58ae1-9177-	A-SPL-SPLU-040424/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			Dashboard Studio app lacks protections for risky SPL commands. This could let attackers bypass SPL safeguards for risky commands in the Hub. The vulnerability would require the attacker to phish the victim by tricking them into initiating a request within their browser. **CVE ID : CVE-2024-29946**	40b8-a26c-8966040f11ae/	
Insertion of Sensitive Information into Log File	27-Mar-2024	7.2	In Splunk Enterprise versions below 9.2.1, 9.1.4, and 9.0.9, the software potentially exposes authentication tokens during the token validation process. This exposure happens when either Splunk Enterprise runs in debug mode or the JsonWebToken component has been configured to log its activity at the DEBUG logging level.	https://advisory.splunk.com/advisories/SVD-2024-0301, https://research.splunk.com/application/9a67e749-d291-40dd-8376-d422e7ecf8b5	A-SPL-SPLU-040424/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-29945		
Affected Version(s): From (including) 9.1.0 Up to (excluding) 9.1.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Mar-2024	8.1	In Splunk Enterprise versions below 9.2.1, 9.1.4, and 9.0.9, the Dashboard Examples Hub in the Splunk Dashboard Studio app lacks protections for risky SPL commands. This could let attackers bypass SPL safeguards for risky commands in the Hub. The vulnerability would require the attacker to phish the victim by tricking them into initiating a request within their browser. **CVE ID : CVE-2024-29946**	https://advisory.splunk.com/advisories/SVD-2024-0302, https://research.splunk.com/application/1cf58ae1-9177-40b8-a26c-8966040f11ae/	A-SPL-SPLU-040424/42
Insertion of Sensitive Information into Log File	27-Mar-2024	7.2	In Splunk Enterprise versions below 9.2.1, 9.1.4, and 9.0.9, the software potentially exposes authentication tokens during the token validation process. This exposure happens	https://advisory.splunk.com/advisories/SVD-2024-0301, https://research.splunk.com/application/9a67e749-d291-40dd-8376-d422e7ecf8b5	A-SPL-SPLU-040424/43

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when either Splunk Enterprise runs in debug mode or the JsonWebToken component has been configured to log its activity at the DEBUG logging level. **CVE ID : CVE-2024-29945**		
Affected Version(s): From (including) 9.2.0 Up to (excluding) 9.2.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Mar-2024	8.1	In Splunk Enterprise versions below 9.2.1, 9.1.4, and 9.0.9, the Dashboard Examples Hub in the Splunk Dashboard Studio app lacks protections for risky SPL commands. This could let attackers bypass SPL safeguards for risky commands in the Hub. The vulnerability would require the attacker to phish the victim by tricking them into initiating a request within their browser. **CVE ID : CVE-2024-29946**	https://advisory.splunk.com/advisories/SVD-2024-0302, https://research.splunk.com/application/1cf58ae1-9177-40b8-a26c-8966040f11ae/	A-SPL-SPLU-040424/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	27-Mar-2024	7.2	In Splunk Enterprise versions below 9.2.1, 9.1.4, and 9.0.9, the software potentially exposes authentication tokens during the token validation process. This exposure happens when either Splunk Enterprise runs in debug mode or the JsonWebToken component has been configured to log its activity at the DEBUG logging level. **CVE ID : CVE-2024-29945**	https://advisory.splunk.com/advisories/SVD-2024-0301, https://research.splunk.com/application/9a67e749-d291-40dd-8376-d422e7ecf8b5	A-SPL-SPLU-040424/45
Vendor: tukaani					
Product: xz					
Affected Version(s): 5.6.0					
Embedded Malicious Code	29-Mar-2024	10	Malicious code was discovered in the upstream tarballs of xz, starting with version 5.6.0. Through a series of complex obfuscations, the liblzma build process extracts a prebuilt object file from a disguised test file existing in the source code,	https://access.redhat.com/security/cve/CVE-2024-3094, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1068024, https://bugzilla.redhat.com/show_bug.cgi?id=2272210, https://tukaani	A-TUK-XZ-040424/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is then used to modify specific functions in the liblzma code. This results in a modified liblzma library that can be used by any software linked against this library, intercepting and modifying the data interaction with this library. **CVE ID : CVE-2024-3094**	.org/xz-backdoor/	
Affected Version(s): 5.6.1					
Embedded Malicious Code	29-Mar-2024	10	Malicious code was discovered in the upstream tarballs of xz, starting with version 5.6.0. Through a series of complex obfuscations, the liblzma build process extracts a prebuilt object file from a disguised test file existing in the source code, which is then used to modify specific functions in the liblzma code. This results in a modified liblzma library that can be used by any software linked against this	https://access.redhat.com/security/cve/CVE-2024-3094, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1068024, https://bugzilla.redhat.com/show_bug.cgi?id=2272210, https://tukaani.org/xz-backdoor/	A-TUK-XZ-040424/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			library, intercepting and modifying the data interaction with this library. **CVE ID : CVE-2024-3094**		
Hardware					
Vendor: Tenda					
Product: ac10					
Affected Version(s): 4.0					
Stack-based Buffer Overflow	24-Mar-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda AC10 16.03.10.13/16.03.10.20. Affected by this issue is the function fromSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument timeZone 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-257780. NOTE: The vendor was contacted	N/A	H-TEN-AC10-040424/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2856**		
Product: ac10u					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-2024	9.8	A vulnerability was found in Tenda AC10U 15.03.06.48/15.03.06.49. It has been rated as critical. This issue affects the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257777 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	H-TEN-AC10-040424/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-2853		
Product: ac15					
Affected Version(s): 1.0					
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability classified as critical has been found in Tenda AC15 15.03.05.18/15.03.20_multi. This affects the function addWifiMacFilter of the file /goform/addWifiMacFilter. The manipulation of the argument deviceId/deviceMac 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. The identifier VDB-257661 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2806**	N/A	H-TEN-AC15-040424/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability classified as critical was found in Tenda AC15 15.03.05.18/15.03.20_multi. This vulnerability affects the function formExpandDlnaFile of the file /goform/expandDlnaFile. The manipulation of the argument filePath 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-257662 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-2024-2807**	N/A	H-TEN-AC15-040424/51
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda AC15 15.03.05.18/15.03	N/A	H-TEN-AC15-040424/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			.20_multi. This issue affects the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. 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-257663. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2808**		
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability, which was classified as critical, was found in Tenda AC15 15.03.05.18/15.03.20_multi. Affected is the function formSetFirewallCfg of the file /goform/SetFirewallCfg. The	N/A	H-TEN-AC15-040424/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument firewallEn 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. The identifier of this vulnerability is VDB-257664. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2809**		
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability has been found in Tenda AC15 15.03.05.18/15.03.20_multi and classified as critical. Affected by this vulnerability is the function formWifiWpsOOB of the file /goform/WifiWpsOOB. The manipulation of the argument index leads to stack-based buffer overflow. The attack can be	N/A	H-TEN-AC15-040424/54

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-257665 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2810**		
Stack-based Buffer Overflow	24-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.20_multi. It has been declared as critical. This vulnerability affects the function saveParentControlInfo of the file /goform/saveParentControlInfo. The manipulation of the argument urls leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this	N/A	H-TEN-AC15-040424/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-257776. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2852**		
Stack-based Buffer Overflow	24-Mar-2024	9.8	A vulnerability classified as critical was found in Tenda AC15 15.03.05.18/15.03.05.19/15.03.20. Affected by this vulnerability is the function fromSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument time leads to stack-based buffer overflow. 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-257779. NOTE: The vendor was contacted early about this disclosure but did	N/A	H-TEN-AC15-040424/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2024-2855**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Mar-2024	8.8	A vulnerability was found in Tenda AC15 15.03.05.18/15.03.20_multi. It has been classified as critical. This affects the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac 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 associated identifier of this vulnerability is VDB-257667. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2812**	N/A	H-TEN-AC15-040424/57
Affected Version(s): -					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.20_multi and classified as critical. Affected by this issue is the function formWifiWpsStart of the file /goform/WifiWpsStart. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257666 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-2024-2811**	N/A	H-TEN-AC15-040424/58
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.20_multi. It has been declared as critical. This vulnerability	N/A	H-TEN-AC15-040424/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects the function form_fast_setting_wifi_set of the file /goform/fast_setting_wifi_set. The manipulation of the argument ssid leads to stack-based 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-257668. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2813**		
N/A	22-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.20_multi. It has been rated as critical. This issue affects the function fromDhcpListClient of the file /goform/DhcpListClient. The manipulation of the argument page leads to	N/A	H-TEN-AC15-040424/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257669 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2814**		
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability classified as critical has been found in Tenda AC15 15.03.20_multi. Affected is the function R7WebsSecurityHandler of the file /goform/execCommand of the component Cookie Handler. The manipulation of the argument password leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been	N/A	H-TEN-AC15-040424/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. VDB-257670 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-2024-2815**		
Stack-based Buffer Overflow	24-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.05.18 and classified as critical. Affected by this issue is the function saveParentControlInfo of the file /goform/saveParentControlInfo. The manipulation of the argument urls leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257774 is the identifier assigned to this vulnerability.	N/A	H-TEN-AC15-040424/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2850**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.05.18/15.03.20_multi. It has been classified as critical. This affects the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName 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 associated identifier of this vulnerability is VDB-257775. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	H-TEN-AC15-040424/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-2851		
Cross-Site Request Forgery (CSRF)	22-Mar-2024	6.5	A vulnerability classified as problematic was found in Tenda AC15 15.03.05.18. Affected by this vulnerability is the function fromSysToolReboot of the file /goform/SysToolReboot. 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 associated identifier of this vulnerability is VDB-257671. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2816**	N/A	H-TEN-AC15-040424/64
Cross-Site Request Forgery (CSRF)	22-Mar-2024	6.5	A vulnerability, which was classified as problematic, has been found in Tenda AC15 15.03.05.18.	N/A	H-TEN-AC15-040424/65

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected by this issue is the function fromSysToolRestoreSet of the file /goform/SysToolRestoreSet. The manipulation leads to cross-site request forgery. 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-257672. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2817**		
Product: ac18					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-2024	9.8	A vulnerability classified as critical has been found in Tenda AC18 15.03.05.05. Affected is the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument	N/A	H-TEN-AC18-040424/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			usbName leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257778 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-2024-2854**		
Operating System					
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 38					
N/A	20-Mar-2024	8.8	Object lifecycle issue in V8 in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-2625		
Use After Free	20-Mar-2024	8.8	Use after free in Canvas in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2627**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/68
Out-of-bounds Read	20-Mar-2024	6.5	Out of bounds read in Swiftshader in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2626**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/69
N/A	20-Mar-2024	6.5	Inappropriate implementation in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to leak cross-origin data	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2630**		
N/A	20-Mar-2024	4.3	Inappropriate implementation in Downloads in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted URL. (Chromium security severity: Medium) **CVE ID : CVE-2024-2628**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/71
N/A	20-Mar-2024	4.3	Incorrect security UI in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2629**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/72
N/A	20-Mar-2024	4.3	Inappropriate implementation in iOS in Google Chrome prior to 123.0.6312.58	https://chromereleases.googleblog.com/2024/03/stable-channel-	O-FED-FEDO-040424/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2024-2631**	update-for-desktop_19.html	
Affected Version(s): 39					
N/A	20-Mar-2024	8.8	Object lifecycle issue in V8 in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-2625**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/74
Use After Free	20-Mar-2024	8.8	Use after free in Canvas in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2627**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Mar-2024	6.5	Out of bounds read in Swiftshader in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2626**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/76
N/A	20-Mar-2024	6.5	Inappropriate implementation in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2630**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/77
N/A	20-Mar-2024	4.3	Inappropriate implementation in Downloads in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted URL.	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/78

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: Medium) **CVE ID : CVE-2024-2628**		
N/A	20-Mar-2024	4.3	Incorrect security UI in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2629**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/79
N/A	20-Mar-2024	4.3	Inappropriate implementation in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2024-2631**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/80
Affected Version(s): 40					
N/A	20-Mar-2024	8.8	Object lifecycle issue in V8 in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-	O-FED-FEDO-040424/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-2625**	desktop_19.html	
Use After Free	20-Mar-2024	8.8	Use after free in Canvas in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2627**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/82
Out-of-bounds Read	20-Mar-2024	6.5	Out of bounds read in Swiftshader in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2626**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Mar-2024	6.5	Inappropriate implementation in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-2630**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/84
N/A	20-Mar-2024	4.3	Inappropriate implementation in Downloads in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted URL. (Chromium security severity: Medium) **CVE ID : CVE-2024-2628**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/85
N/A	20-Mar-2024	4.3	Incorrect security UI in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: Medium) **CVE ID : CVE-2024-2629**		
N/A	20-Mar-2024	4.3	Inappropriate implementation in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2024-2631**	https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html	O-FED-FEDO-040424/87
Vendor: Tenda					
Product: ac10u_firmware					
Affected Version(s): 15.03.06.48					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-2024	9.8	A vulnerability was found in Tenda AC10U 15.03.06.48/15.03.06.49. It has been rated as critical. This issue affects the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. The attack may be initiated remotely. The exploit has	N/A	O-TEN-AC10-040424/88

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. The identifier VDB-257777 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2853**		
Affected Version(s): 15.03.06.49					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-2024	9.8	A vulnerability was found in Tenda AC10U 15.03.06.48/15.03.06.49. It has been rated as critical. This issue affects the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257777 was assigned to this vulnerability.	N/A	O-TEN-AC10-040424/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2853**		
Product: ac10_firmware					
Affected Version(s): 16.03.10.13					
Stack-based Buffer Overflow	24-Mar-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda AC10 16.03.10.13/16.03.10.20. Affected by this issue is the function fromSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument timeZone 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-257780. NOTE: The vendor was contacted early about this disclosure but did	N/A	O-TEN-AC10-040424/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2024-2856**		
Affected Version(s): 16.03.10.20					
Stack-based Buffer Overflow	24-Mar-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda AC10 16.03.10.13/16.03.10.20. Affected by this issue is the function fromSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument timeZone 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-257780. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2856**	N/A	O-TEN-AC10-040424/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ac15_firmware					
Affected Version(s): 15.03.05.18					
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability classified as critical has been found in Tenda AC15 15.03.05.18/15.03.20_multi. This affects the function addWifiMacFilter of the file /goform/addWifiMacFilter. The manipulation of the argument deviceId/deviceMac 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. The identifier VDB-257661 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2806**	N/A	O-TEN-AC15-040424/92
Stack-based	22-Mar-2024	9.8	A vulnerability classified as critical was found	N/A	O-TEN-AC15-040424/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			in Tenda AC15 15.03.05.18/15.03.20_multi. This vulnerability affects the function formExpandDlnaFile of the file /goform/expandDlnaFile. The manipulation of the argument filePath 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-257662 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-2024-2807**		
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda AC15 15.03.05.18/15.03.20_multi. This issue affects the function	N/A	O-TEN-AC15-040424/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. 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-257663. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2808**		
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability, which was classified as critical, was found in Tenda AC15 15.03.05.18/15.03.20_multi. Affected is the function formSetFirewallCfg of the file /goform/SetFirewallCfg. The manipulation of the argument firewallEn leads	N/A	O-TEN-AC15-040424/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. The identifier of this vulnerability is VDB-257664. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2809**		
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability has been found in Tenda AC15 15.03.05.18/15.03.20_multi and classified as critical. Affected by this vulnerability is the function formWifiWpsOOB of the file /goform/WifiWpsOOB. The manipulation of the argument index leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been	N/A	O-TEN-AC15-040424/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. The identifier VDB-257665 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2810**		
Stack-based Buffer Overflow	24-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.05.18 and classified as critical. Affected by this issue is the function saveParentControlInfo of the file /goform/saveParentControlInfo. The manipulation of the argument urls leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257774 is the identifier assigned to this vulnerability.	N/A	O-TEN-AC15-040424/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2850**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.05.18/15.03.20_multi. It has been classified as critical. This affects the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName 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 associated identifier of this vulnerability is VDB-257775. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	O-TEN-AC15-040424/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-2851		
Stack-based Buffer Overflow	24-Mar-2024	9.8	A vulnerability classified as critical was found in Tenda AC15 15.03.05.18/15.03.05.19/15.03.20. Affected by this vulnerability is the function fromSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument time leads to stack-based buffer overflow. 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-257779. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2855**	N/A	O-TEN-AC15-040424/99
Improper Neutralization of Special	22-Mar-2024	8.8	A vulnerability was found in Tenda AC15 15.03.05.18/15.03	N/A	O-TEN-AC15-040424/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			.20_multi. It has been classified as critical. This affects the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac 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 associated identifier of this vulnerability is VDB-257667. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2812**		
Cross-Site Request Forgery (CSRF)	22-Mar-2024	6.5	A vulnerability classified as problematic was found in Tenda AC15 15.03.05.18. Affected by this vulnerability is the function fromSysToolReboot of the file	N/A	O-TEN-AC15-040424/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/goform/SysToolReboot. 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 associated identifier of this vulnerability is VDB-257671. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2816**		
Cross-Site Request Forgery (CSRF)	22-Mar-2024	6.5	A vulnerability, which was classified as problematic, has been found in Tenda AC15 15.03.05.18. Affected by this issue is the function fromSysToolRestoreSet of the file /goform/SysToolRestoreSet. The manipulation leads to cross-site request forgery. The attack may be launched	N/A	O-TEN-AC15-040424/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257672. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2817**		
Affected Version(s): 15.03.05.19					
Stack-based Buffer Overflow	24-Mar-2024	9.8	A vulnerability classified as critical was found in Tenda AC15 15.03.05.18/15.03.05.19/15.03.20. Affected by this vulnerability is the function fromSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument time leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated	N/A	O-TEN-AC15-040424/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier of this vulnerability is VDB-257779. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2855**		
Affected Version(s): 15.03.05.20_multi					
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability classified as critical has been found in Tenda AC15 15.03.05.18/15.03.20_multi. This affects the function addWifiMacFilter of the file /goform/addWifiMacFilter. The manipulation of the argument deviceId/deviceMac 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. The identifier VDB-257661 was assigned to this vulnerability. NOTE: The vendor	N/A	O-TEN-AC15-040424/104

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-2024-2806**		
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability classified as critical was found in Tenda AC15 15.03.05.18/15.03.20_multi. This vulnerability affects the function formExpandDlnaFile of the file /goform/expandDlnaFile. The manipulation of the argument filePath 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-257662 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-2024-2807**	N/A	O-TEN-AC15-040424/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda AC15 15.03.05.18/15.03.20_multi. This issue affects the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. 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-257663. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2808**	N/A	O-TEN-AC15-040424/106
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability, which was classified as critical, was found in Tenda AC15	N/A	O-TEN-AC15-040424/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.03.05.18/15.03.20_multi. Affected is the function formSetFirewallCfg of the file /goform/SetFirewallCfg. The manipulation of the argument firewallEn 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. The identifier of this vulnerability is VDB-257664. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2809**		
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability has been found in Tenda AC15 15.03.05.18/15.03.20_multi and classified as critical. Affected by this vulnerability is the function formWifiWpsOOB of the file /goform/WifiWps	N/A	O-TEN-AC15-040424/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OOB. The manipulation of the argument index leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257665 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2810**		
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.20_multi and classified as critical. Affected by this issue is the function formWifiWpsStart of the file /goform/WifiWpsStart. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be	N/A	O-TEN-AC15-040424/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launched remotely. The exploit has been disclosed to the public and may be used. VDB-257666 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-2024-2811**		
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.20_multi. It has been declared as critical. This vulnerability affects the function form_fast_setting_wifi_set of the file /goform/fast_setting_wifi_set. The manipulation of the argument ssid leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this	N/A	O-TEN-AC15-040424/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-257668. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2813**		
N/A	22-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.20_multi. It has been rated as critical. This issue affects the function fromDhcpListClient of the file /goform/DhcpListClient. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257669 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	O-TEN-AC15-040424/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-2814		
Stack-based Buffer Overflow	22-Mar-2024	9.8	A vulnerability classified as critical has been found in Tenda AC15 15.03.20_multi. Affected is the function R7WebsSecurityHandler of the file /goform/execCommand of the component Cookie Handler. The manipulation of the argument password 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. VDB-257670 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-2024-2815**	N/A	O-TEN-AC15-040424/112
Improper Neutralization of	22-Mar-2024	8.8	A vulnerability was found in Tenda AC15	N/A	O-TEN-AC15-040424/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			15.03.05.18/15.03.20_multi. It has been classified as critical. This affects the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac 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 associated identifier of this vulnerability is VDB-257667. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2812**		
Affected Version(s): 15.03.20_multi					
Improper Neutralization of Special Elements used in an OS Command	24-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.05.18/15.03.20_multi. It has been classified as critical. This affects the	N/A	O-TEN-AC15-040424/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName 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 associated identifier of this vulnerability is VDB-257775. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2851**		
Stack-based Buffer Overflow	24-Mar-2024	9.8	A vulnerability was found in Tenda AC15 15.03.20_multi. It has been declared as critical. This vulnerability affects the function saveParentControlInfo of the file /goform/saveParentControlInfo. The manipulation of	N/A	O-TEN-AC15-040424/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the argument urls leads to stack-based 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-257776. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2852**		
Stack-based Buffer Overflow	24-Mar-2024	9.8	A vulnerability classified as critical was found in Tenda AC15 15.03.05.18/15.03.05.19/15.03.20. Affected by this vulnerability is the function fromSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument time leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been	N/A	O-TEN-AC15-040424/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257779. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-2855**		
Product: ac18_firmware					
Affected Version(s): 15.03.05.05					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-2024	9.8	A vulnerability classified as critical has been found in Tenda AC18 15.03.05.05. Affected is the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257778 is the identifier assigned to this	N/A	O-TEN-AC18-040424/117

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-2024-2854**		