

National Critical Information Infrastructure Protection Centre Common Vulnerabilities and Exposures (CVE) Report

16 - 31 Mar 2024

of Comb

Tabl

Vol. 11 No. 06

Table of Content							
Vendor	Page Number						
Application							
deltaww	diaenergie	1					
Google	chrome	1					
	cics_transaction_gateway	4					
	cloud_pak_for_business_automation	5					
	infosphere_information_server	15					
IBM	security_verify_access	16					
	security_verify_directory	16					
	storage_protect_plus	18					
	websphere_application_server	18					
ivanti	neurons_for_itsm	19					
Ivanci	standalone_sentry	19					
Microsoft	edge	20					
Splunk	splunk	20					
tukaani	XZ	24					
Hardware							
	ac10	26					
Tenda	ac10u	27					
i ciiua	ac15	28					
	ac18	41					
Operating System							
Fedoraproject	fedora	42					
	ac10u_firmware	50					
Tenda	ac10_firmware	52					
	ac15_firmware	54					
	ac18_firmware	75					

Common Vulnerabilities and Exposures (CVE) Report							
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			Application				
Vendor: del	taww						
Product: dia							
Affected Ver	sion(s): * Up to (e	excluding)		I			
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.	N/A	A-DEL-DIAE- 040424/1		
Vendor: Go	-		CVE ID : CVE- 2024-28029				
Product: ch							
Affected Ver	sion(s): * Up to (e	excluding					
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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	A-GOO-CHRO- 040424/2		
			CVE ID : CVE- 2024-2625				

0-1

5-6

6-7

7-8

2-3

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)	https://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	A-GOO-CHRO- 040424/3
			CVE ID : CVE- 2024-2627 Out of bounds		
Out-of- bounds Read	20-Mar-2024	6.5	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)	https://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	A-GOO-CHRO- 040424/4
			CVE ID : CVE- 2024-2626		
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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	A-GOO-CHRO- 040424/5

0-1

5-6

6-7

7-8

8-9

9-10

2-3

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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	A-GOO-CHRO- 040424/7

0-1

5-6

2-3

1-2

6-7 7-8 8-9

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)	https://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	A-GOO-CHRO- 040424/8
			CVE ID : CVE- 2024-2631		
Vendor: IBM	1				
	s_transaction_g	ateway			
Affected Ver	sion(s): 9.2	1	1		
Insufficient ly 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.	https://https// www.ibm.com/ support/pages/ node/7145418	A-IBM-CICS- 040424/9
Affected Vers	sion(s): 9.3		CVE ID : CVE- 2023-50311		

0-1

3-4 4-5 Page **4** of **76** 5-6

6-7

7-8

2-3

1-2

8-9 **9-10**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient ly 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: clo	oud_pak_for_bus	iness_aut	comation		
Affected Ver	sion(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, 22.0.1,2 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.	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	A-IBM-CLOU- 040424/11

0-1

3-4 4-5 Page **5** of **76**

2-3

1-2

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 275938. CVE ID : CVE- 2023-50959		
Affected Ver	sion(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, 22.0.1,2 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-	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	A-IBM-CLOU- 040424/12
Affected Ver	sion(s): 18.0.2		2023-50959		
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://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	A-IBM-CLOU- 040424/13

0-1

5-6

6-7

7-8

8-9

9-10

2-3

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 Ver	sion(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, 22.0.1,2 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.	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	A-IBM-CLOU- 040424/14

0-1

5-6

2-3

1-2

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2023-50959		
Affected Ver	sion(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, 22.0.1,2 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	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	A-IBM-CLOU- 040424/15
Affected Ver	sion(s): 19.0.3			1	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, 22.0.1,2 2.0.2, 23.0.1, and 23.0.2 may allow	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	A-IBM-CLOU- 040424/16

0-1

3-4 4-5 Page **8** of **76**

5-6

6-7

2-3

1-2

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 Ver	sion(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, 22.0.1,2 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	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	A-IBM-CLOU- 040424/17
Affects of Maria	aion(a), 20.0.2		2023-50959		
Affected Ver	sion(s): 20.0.2				

0-1

5-6

2-3

1-2

6-7 7-8 8-9

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, 22.0.1,2 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-	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	A-IBM-CLOU- 040424/18
Affected Ver	sion(s): 20.0.3		2023-50959		
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 2.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	A-IBM-CLOU- 040424/19

0-1

1-2

2-3

3-4 4-5 Page **10** of **76** 5-6

7-8

6-7

8-9 9-10

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 Ver	sion(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, 22.0.1,2 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	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	A-IBM-CLOU- 040424/20
Affected Ver	sion(s): 21.0.2				
N/A	31-Mar-2024	6.5	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1,	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759	A-IBM-CLOU- 040424/21

	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6
--	--------------------	-----	-----	-----	-----	-----	-----

6-7

7-8

8-9

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, 22.0.1,2 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	38, https://www.ib m.com/support /pages/node/7 145492	
Affected Ver	sion(s): 21.0.3		2023-50959		
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 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	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	A-IBM-CLOU- 040424/22

0-1

1-2

2-3

3-4 4-5 Page **12** of **76** 6-7 7-8

5-6

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 Ver	sion(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, 22.0.1,2 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	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	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://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support	A-IBM-CLOU- 040424/24			

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Page **14** of **76**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID : CVE- 2023-50959						
Affected Ver	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, 22.0.1,2 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	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2759 38, https://www.ib m.com/support /pages/node/7 145492	A-IBM-CLOU- 040424/26				
Product: inf	f <mark>osphere_inform</mark>	nation_se	rver	<u> </u>	<u> </u>				
Affected Ver	sion(s): 11.7								
Insertion of Sensitive Informatio n 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://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2803 61, https://www.ib m.com/support /pages/node/7 117184	A-IBM-INFO- 040424/27				

0-1

1-2

2-3

3-4 4-5 Page **15** of **76** 5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID : CVE- 2024-22352						
Product: see	Product: security_verify_access								
Affected Ver	sion(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://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2816 07, https://www.ib m.com/support /pages/node/7 145400	A-IBM-SECU- 040424/28				
Product: see	curity_verify_di	rectory	I						
Affected Ver	sion(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://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2284 44, https://www.ib m.com/support /pages/node/7 145001	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://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2284 37, https://www.ib m.com/support	A-IBM-SECU- 040424/30				

0-1

1-2

2-3

3-4 4-5 Page **16** of **76** 5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			further attacks against the system. IBM X- Force ID: 228437.	/pages/node/7 145001	
			CVE ID : CVE- 2022-32751		
Improper Neutralizat ion 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.	https://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2284 45, https://www.ib m.com/support /pages/node/7 145001	A-IBM-SECU- 040424/31
			CVE ID : CVE- 2022-32754		
Generation of Error Message Containing Sensitive Informatio n	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://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2285 07, https://www.ib m.com/support /pages/node/7 145001	A-IBM-SECU- 040424/32

0-1

1-2

2-3

3-4 4-5 Page **17** of **76** 6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. IBM X- Force ID: 228507.		
			CVE ID : CVE- 2022-32756		
Product: sto	orage_protect_p	lus			
Affected Ver	sion(s): From (in	cluding) 1	0.1.0 Up to (includin	g) 10.1.16	
Improper Privilege Manageme nt	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://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2715 38, https://www.ib m.com/support /pages/node/7 144861	A-IBM-STOR- 040424/33
Product: we	bsphere_applic	ation_ser	ver		
Affected Ver	sion(s): From (in	cluding) 1	7.0.0.3 Up to (includ	ing) 24.0.0.3	
Uncontroll ed Resource Consumpti on	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://exchan ge.xforce.ibmcl oud.com/vulne rabilities/2804 00, https://www.ib m.com/support /pages/node/7 145365	A-IBM-WEBS- 040424/34

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			resources. IBM X- Force ID: 280400.					
			CVE ID : CVE- 2024-22353					
Vendor: iva	nti							
Product: neurons_for_itsm								
Affected Ver	sion(s): * Up to (e	excluding)		[Γ			
Unrestricte d 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/ar ticle/SA-CVE- 2023-46808- Authenticated- Remote-File- Write-for- Ivanti-Neurons- for-ITSM	A-IVA-NEUR- 040424/35			
	andalone_sentry sion(s): * Up to (e		9.19.0					
Improper Neutralizat ion of Special Elements used in a Command ('Comman d 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/ar ticle/CVE- 2023-41724- Remote-Code- Execution-for- Ivanti- Standalone- Sentry	A-IVA-STAN- 040424/36			

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2023-41724		
Vendor: Mi	crosoft				
Product: ed	lge				
Affected Ver	sion(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.m icrosoft.com/u pdate- guide/vulnerab ility/CVE-2024- 26196	A-MIC-EDGE- 040424/37
Affected Ver	sion(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.m icrosoft.com/u pdate- guide/vulnerab ility/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.m icrosoft.com/u pdate- guide/vulnerab ility/CVE-2024- 29057	A-MIC-EDGE- 040424/39
Vendor: Spl	unk				
Product: sp	lunk				
Affected Ver	sion(s): From (in	cluding) 9	0.0.0 Up to (excluding) 9.0.9	
Improper Neutralizat ion 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://advisor y.splunk.com/a dvisories/SVD- 2024-0302, https://researc h.splunk.com/a pplication/1cf5 8ae1-9177-	A-SPL-SPLU- 040424/40

0-1

1-2

2-3

5-6

6-7

7-8

8-9

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 Informatio n 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://advisor y.splunk.com/a dvisories/SVD- 2024-0301, https://researc h.splunk.com/a pplication/9a6 7e749-d291- 40dd-8376- d422e7ecf8b5	A-SPL-SPLU- 040424/41

0-1

1-2

2-3

3-4 4-5 Page **21** of **76** 6-7 7-8

5-6

9-10

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 Neutralizat ion of Special Elements used in a Command ('Comman d 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-	https://advisor y.splunk.com/a dvisories/SVD- 2024-0302, https://researc h.splunk.com/a pplication/1cf5 8ae1-9177- 40b8-a26c- 8966040f11ae/	A-SPL-SPLU- 040424/42			
Insertion of Sensitive Informatio n into Log File	27-Mar-2024	7.2	2024-29946 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://advisor y.splunk.com/a dvisories/SVD- 2024-0301, https://researc h.splunk.com/a pplication/9a6 7e749-d291- 40dd-8376- d422e7ecf8b5	A-SPL-SPLU- 040424/43			

0-1

1-2

2-3

3-4 4-5 Page **22** of **76**

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): From (in	cluding) 9	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	9.2.1	
			In Splunk		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	27-Mar-2024	8.1	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://advisor y.splunk.com/a dvisories/SVD- 2024-0302, https://researc h.splunk.com/a pplication/1cf5 8ae1-9177- 40b8-a26c- 8966040f11ae/	A-SPL-SPLU- 040424/44

0-1

1-2

2-3

3-4 4-5 Page **23** of **76** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Informatio n 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://advisor y.splunk.com/a dvisories/SVD- 2024-0301, https://researc h.splunk.com/a pplication/9a6 7e749-d291- 40dd-8376- d422e7ecf8b5	A-SPL-SPLU- 040424/45
Vendor: tuk					
Product: xz					
Affected Ver	sion(s): 5.6.0			r	
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.r edhat.com/secu rity/cve/CVE- 2024-3094, https://bugs.de bian.org/cgi- bin/bugreport.c gi?bug=106802 4, https://bugzilla .redhat.com/sh ow_bug.cgi?id= 2272210, https://tukaani	A-TUK-XZ- 040424/46

0-1

1-2

2-3

5-6

6-7

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 Ver	sion(s): 5.6.1		L		I
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.r edhat.com/secu rity/cve/CVE- 2024-3094, https://bugs.de bian.org/cgi- bin/bugreport.c gi?bug=106802 4, https://bugzilla .redhat.com/sh ow_bug.cgi?id= 2272210, https://tukaani .org/xz- backdoor/	A-TUK-XZ- 040424/47

0-1

1-2

2-3

3-4 4-5 Page **25** of **76** 5-6

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: Ter	nda				
Product: ac					
Affected Ver	sion(s): 4.0			Γ	
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/SetSysTi meCfg. 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

0-1

1-2

2-3

3-4 4-5 Page **26** of **76** 7-8

6-7

5-6

8-9 9-10

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: ac	10u				
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion 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 formSetSambaCon f of the file /goform/setsamb acfg. 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

0-1

1-2

2-3

3-4 4-5 Page **27** of **76** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-2853		
Product: ac	15				
Affected Ver	rsion(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/addWifi MacFilter. The manipulation of the argument deviceId/deviceM ac 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

0-1

1-2

2-3

3-4 4-5 Page **28** of **76** 5-6

6-7

7-8 8-9

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 formExpandDlnaF ile of the file /goform/expandD lnaFile. 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

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			.20_multi. This issue affects the function formQuickIndex of the file /goform/QuickIn dex. 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 formSetFirewallCf g of the file /goform/SetFirew allCfg. The	N/A	H-TEN-AC15- 040424/53

0-1

1-2

2-3

3-4 4-5 Page **30** of **76** 5-6

6-7

7-8

8-9

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/WifiWps OOB. The manipulation of the argument index leads to stack-based buffer overflow. The attack can be	N/A	H-TEN-AC15- 040424/54

0-1

1-2

2-3

3-4 4-5 Page **31** of **76** 6-7 7-8

5-6

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 saveParentContro lInfo of the file /goform/savePare ntControlInfo. 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

0-1

1-2

2-3

3-4 4-5 Page **32** of **76** 6-7 7-8

5-6

9-10

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.		
Stack- based Buffer Overflow	24-Mar-2024	9.8	any way. CVE ID : CVE- 2024-2852 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/SetSysTi meCfg. 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	N/A	H-TEN-AC15- 040424/56

0-1

1-2

2-3

3-4 4-5 Page **33** of **76** 6-7 7-8

5-6

9-10

Improper Neutralizati ion of Special Elements used in any 22-Mar-2024AA vulnerability was found in Tenda AC15 15.03.05.18/15.03 .20,mult.1 thas been classified as critical. This affects the function formWriteFacMac of the file /goform/WriteFa cMac.The manipulation of the argument mac leads to os command ligiction']H-TEN-AC15- 040424/57Improper Neutralizat ion of Special Elements used in an (OS Command ligiction')22-Mar-20248.8N/AH-TEN-AC15- 040424/57VB-TEN-AC15- mothers value injection in the associated identifier of this vulnerability is VDB-257667. NOTE: The vendor was contacted idisclosure but did not respond in anyway.N/AH-TEN-AC15- 040424/57	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements Used in an of Special Elements Used in an injection')22-Mar-20248.8Base Neutralization of the argument mac injection. It is possible to initiate the attack remody. The associated identifier of this vulnerability is VDB-257667. NOTE: The vendor was contacted early about this disclosed to the public and maybe used. The associated identifier of this vulnerability is VDB-257667. NOTE: The vendor was contacted early about this disclosed to the public and maybe used. The associated identifier of this vulnerability is VDB-257667.N/AH-TEN-AC15- 040424/57				any way. CVE ID : CVE-		
Affected Version(s): -	Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')		8.8	<pre>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/WriteFa cMac. 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.</pre>	N/A	

0-1

1-2

2-3

5-6

6-7 7-8

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/WifiWps Start. 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

0-1

5-6

6-7

2-3

1-2

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects the function form_fast_setting_ wifi_set of the file /goform/fast_setti ng_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 fromDhcpListClie nt of the file /goform/DhcpList Client. The manipulation of the argument page leads to	N/A	H-TEN-AC15- 040424/60

0-1

1-2

2-3

3-4 4-5 Page **36** of **76** 6-7 7-8

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 R7WebsSecurityH andler of the file /goform/execCom mand of the file /goform/execCom mand of the file 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

0-1

1-2

2-3

3-4 4-5 Page **37** of **76** 6-7 7-8

5-6

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 saveParentContro lInfo of the file /goform/savePare ntControlInfo. 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

0-1

1-2

2-3

3-4 4-5 Page **38** of **76** 6-7 7-8

5-6

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-		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-2024	9.8	2024-2850 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 formSetSambaCon f of the file /goform/setsamb acfg. 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

0-1

1-2

2-3

3-4 4-5 Page **39** of **76** 6-7 7-8

5-6

9-10

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 fromSysToolRebo ot of the file /goform/SysTool Reboot. 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

0-1

1-2

2-3

5-6

6-7

		CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected by this issue is the function fromSysToolResto reSet of the file /goform/SysTool RestoreSet. 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	8				
Affected Version	on(s): -				
Improper Neutralizat ion 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 formSetSambaCon f of the file /goform/setsamb acfg. The manipulation of the argument	N/A	H-TEN-AC18- 040424/66
CVSS Scoring Sca	ale 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
			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		
Vendor: Fed	lovonvoiost	(Operating System		
Product: fee					
Affected Ver					
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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	O-FED-FEDO- 040424/67

0-1

1-2

2-3

5-6

6-7

7-8 8-9

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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	0-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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	0-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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	O-FED-FEDO- 040424/70

0-1

1-2

2-3

3-4 4-5 Page **43** of **76** 5-6

6-7

7-8

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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	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://chrome releases.google blog.com/2024 /03/stable- channel-	O-FED-FEDO- 040424/73

0-1

1-2

2-3

3-4 4-5 Page **44** of **76** 5-6

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)	update-for- desktop_19.htm l	
			CVE ID : CVE- 2024-2631		
Affected Ver	sion(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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	O-FED-FEDO- 040424/75

0-1

1-2

2-3

5-6

6-7

8-9

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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	O-FED-FEDO- 040424/78

0-1

1-2

2-3

3-4 4-5 Page **46** of **76** 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)	https://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	O-FED-FEDO- 040424/79				
			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)	https://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	O-FED-FEDO- 040424/80				
			CVE ID : CVE- 2024-2631						
Affected Ver	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://chrome releases.google blog.com/2024 /03/stable- channel- update-for-	O-FED-FEDO- 040424/81				
				5-6 6-7 7-8	2 20 040				
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5	5-6 6-7 7-8	3 8-9 <mark>9-10</mark>				

Page **47** of **76**

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-	desktop_19.htm l	
			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-	https://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	0-FED-FEDO- 040424/82
Out-of- bounds Read	20-Mar-2024	6.5	2024-2627 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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	O-FED-FEDO- 040424/83

0-1

1-2

2-3

5-6

6-7 7-8 8-9

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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	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://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm l	0-FED-FEDO- 040424/86

0-1

1-2

2-3

5-6

6-7

7-8

9-10

Improper NetronomediationSecurity severity: Medium)Imapropriate implementation in iOS in Google allowed a remote attacker to attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: LOW)https://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm0-FED-FEDO- 0-0-FED-FEDO- 040424/87Vendor: Te-tu-VVPerform UI spoofing via a crafted HTML page. (Chromium security severity: LOW)https://chrome releases.google blog.com/2024 /03/stable- channel- update-for- desktop_19.htm0-FED-FEDO- 0-0-FED-FEDO- 040424/87Vendor: Te-tu-VVVN/A0-FED-FEDO- 0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A20-Mar-20244.3implementation in ioS in Google Chrome prior to 123.0.6312.58 allowed a remote allowed a remote artacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)https://chrome releases.google blog.com/2024 (03/stable- channel- update-for- desktop_19.htm0-FED-FEDO- 040424/87Vendor: TendeVVendor: TendeVProduct: ac1u_firmwareAAffected Ververs(s): 15:03:06-49A vulnerability was found in Tenda AC10U 15:03:06:49.11 has been rated as critical. This issue affectsA vulnerability rende active no 6:49.11 has been rated as critical. This issue affectsImproper Neutralization of Special Elements used in an OS Command (OS Command (OS Command (DS Command Injection The issue affectsN/A0-TEN-AC10- 040424/88				Medium) CVE ID : CVE-		
Vendor: Terter2024-2631offerenceVendor: TerterProduct: actou_firmwareAffected Verson(s): 15.03.06-49.1tsA vulnerability was found in Tenda AC10U 15.03.06.48/15.03 	N/A	20-Mar-2024	4.3	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:	releases.google blog.com/2024 /03/stable- channel- update-for-	
Product: ac10u_firmwareAffected Version(s): 15.03.06.48Affected Version(s): 15.03.06.48A 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 for the file /goform/setsamb acfg. The manipulation of the argument usbName leads to os command lnjection.')O-TEN-AC10- 040424/88						
Affected Version(s): 15.03.06.48Improper Neutralizat ion of Special Elements used in an OS Command [OS Command Injection']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 formSetSambaCon of the file /goform/setsamb acfg. The manipulation of the argument usbName leads to os command injection. The attack may be initiated remotely.O-TEN-AC10- 040424/88						
Improper Neutralizat ion of Special Elements used in an OS Command [njection']24-Mar-20249.8A 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 formSetSambaCon f of the file /goform/setsamb acfg. The manipulation of the argument usbName leads to os command injection. The attack may be initiated remotely.N/AO-TEN-AC10- 040424/88			40			
Improper Neutralizat ion of Special Elements used in an OS Command (IOS Command Injection')24-Mar-20249.8was found in Tenda AC10U 15.03.06.48/15.03 .06.49. It has been rated as critical. This issue affects the function formSetSambaCon f of the file /goform/setsamb acfg. The manipulation of the argument usbName leads to os command injection. The attack may be initiated remotely.N/AO-TEN-AC10- 040424/88	Affected Vers	sion(s): 15.03.06	.48		1	Γ
	Neutralizat ion of Special Elements used in an OS Command ('OS Command	24-Mar-2024	9.8	was found in Tenda AC10U 15.03.06.48/15.03 .06.49. It has been rated as critical. This issue affects the function formSetSambaCon f of the file /goform/setsamb acfg. The manipulation of the argument usbName leads to os command injection. The attack may be	N/A	

Page **50** of **76**

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-		
		4.0	2024-2853		
Affected Ver	sion(s): 15.03.06	.49			
Improper Neutralizat ion 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 formSetSambaCon f of the file /goform/setsamb acfg. 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

0-1

1-2

2-3

3-4 4-5 Page **51** of **76** 6-7 7-8

5-6

8-9

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		
	10_firmware sion(s): 16.03.10	12			
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/SetSysTi meCfg. 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
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 Page 52 of 76	5-6 6-7 7-8	3 8-9 <mark>9-10</mark>

Page **52** of **76**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. CVE ID : CVE- 2024-2856		
Affected Ver	sion(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/SetSysTi meCfg. 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

0-1

1-2

2-3

3-4 4-5 Page **53** of **76** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ac	15_firmware		I	I	I
Affected Ver	sion(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/addWifi MacFilter. The manipulation of the argument deviceId/deviceM ac 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
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 Page 54 of 76	5-6 6-7 7-8	8 8-9 <mark>9-10</mark>

Page **54** of **76**

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 formExpandDlnaF ile of the file /goform/expandD lnaFile. 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

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			formQuickIndex of the file /goform/QuickIn dex. 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 formSetFirewallCf g of the file /goform/SetFirew allCfg. The manipulation of the argument firewallEn leads	N/A	O-TEN-AC15- 040424/95

0-1

1-2

2-3

6-7 7-8

5-6

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/WifiWps OOB. 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

0-1

1-2

2-3

3-4 4-5 Page **57** of **76** 6-7 7-8

5-6

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 saveParentContro lInfo of the file /goform/savePare ntControlInfo. 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

0-1

1-2

2-3

3-4 4-5 Page **58** of **76** 6-7 7-8

5-6

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-		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-2024	9.8	2024-2850 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 formSetSambaCon f of the file /goform/setsamb acfg. 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

0-1

1-2

2-3

3-4 4-5 Page **59** of **76** 6-7 7-8

5-6

9-10

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/SetSysTi meCfg. 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	0-TEN-AC15- 040424/99
Improper Neutralizat ion 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

0-1

1-2

2-3

5-6

6-7

7-8

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/WriteFa cMac. 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 fromSysToolRebo ot of the file	N/A	O-TEN-AC15- 040424/101

0-1

1-2

2-3

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<pre>/goform/SysTool Reboot. 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</pre>		
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 fromSysToolResto reSet of the file /goform/SysTool RestoreSet. The manipulation leads to cross-site request forgery. The attack may be launched	N/A	O-TEN-AC15- 040424/102

0-1

1-2

2-3

3-4 4-5 Page **62** of **76** 5-6

6-7

7-8 8-9

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 Ver	sion(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/SetSysTi meCfg. 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

0-1

1-2

2-3

3-4 4-5 Page **63** of **76** 5-6

7-8

6-7

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 Ver	<mark>sion(s): 15.03.05.</mark>	.20_multi		I	
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/addWifi MacFilter. The manipulation of the argument deviceId/deviceM ac 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	0-TEN-AC15- 040424/104

0-1

1-2

2-3

3-4 4-5 Page **64** of **76** 5-6

7-8

6-7

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 formExpandDlnaF ile of the file /goform/expandD lnaFile. 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

0-1

1-2

2-3

3-4 4-5 Page **65** of **76** 5-6

6-7

7-8

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/QuickIn dex. 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

0-1

1-2

2-3

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.03.05.18/15.03 .20_multi. Affected is the function formSetFirewallCf g of the file /goform/SetFirew allCfg. 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

0-1

1-2

2-3

5-6 6-7 7-8

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/WifiWps Start. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be	N/A	O-TEN-AC15- 040424/109

0-1

1-2

2-3

3-4 4-5 Page **68** of **76** 6-7 7-8

5-6

9-10

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_setti ng_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

0-1

1-2

2-3

3-4 4-5 Page **69** of **76** 6-7 7-8

5-6

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 fromDhcpListClie nt of the file /goform/DhcpList Client. 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

0-1

1-2

2-3

3-4 4-5 Page **70** of **76** 6-7 7-8

5-6

9-10

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 R7WebsSecurityH andler of the file /goform/execCom mand 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 Neutralizat ion of	22-Mar-2024	8.8	A vulnerability was found in Tenda AC15	N/A	O-TEN-AC15- 040424/113

0-1

1-2

2-3

3-4 4-5 Page **71** of **76** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special			15.03.05.18/15.03		
Elements			.20_multi. It has		
used in an			been classified as		
OS			critical. This		
Command			affects the		
('OS			function		
Command			formWriteFacMac		
Injection')			of the file		
			/goform/WriteFa		
			cMac. 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 Ver	<mark>sion(s): 15.03.20</mark>	_multi			
Improper			A vulnerability		
Neutralizat			was found in		
ion of			Tenda AC15		
Special	24 M. 2024	0.0	15.03.05.18/15.03		O-TEN-AC15-
Elements	24-Mar-2024	9.8	.20_multi. It has	N/A	040424/114
used in an			been classified as		, ,
OS			critical. This		
Command			affects the		
Gommanu					

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			function formSetSambaCon f of the file /goform/setsamb acfg. 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 saveParentContro lInfo of the file /goform/savePare ntControlInfo. The manipulation of	N/A	O-TEN-AC15- 040424/115

0-1

1-2

2-3

5-6

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/SetSysTi meCfg. 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

0-1

1-2

2-3

3-4 4-5 Page **74** of **76** 6-7 7-8

5-6

9-10

Improper Neutralizati ion of Special Elements used in an (OS Command (Injection')A vulnerability is VDB-257779. VDTE: The vendor was contacted early about this disclosure but did not respond in any way. CVE D1 : CVE- 2024-2855Improper venterabilityImproper Neutralizati ion of Special Elements used in an (OS Command (Injection')A vulnerability is (Andr-2024A vulnerability classified as critical has been found in Tenda ACI B15:03.05.05.Improper venterability classified as critical has been found in Tenda (ACI B15:03.05.05.05.N/A0-TEN-ACI8- 040424/117Improper Neutralizati used in an (OS Command (Injection')9.8A vulnerability classified as critical has been found in Tenda (ACI B15:00.305.05.05. Affected is the function for the file (goform/setsamb acfg. The manipulation of the argument usbName leads to os command (Injection)0-TEN-ACI8- 040424/117(S Command (Injection)24-Mar-2024 (PAT)9.8N/A (PAT)Improper by the identifier assigned to thisN/A0-TEN-ACI8- 040424/117	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements Used in an OS Command (NS24-Mar-20249.8Avularability classified as critical has been found in Tenda AC18 15.03.05.05. Affected is the function for the file is of of the file is of				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		
Affected Version(s): 15.03.05.05Affected Version(s): 15.03.05.05.A vulnerability classified as critical has been found in Tenda AC18 15.03.05.05.Affected is the function formSetSambaCon f of the file /goform/setsamb acfg. The manipulation of the argument used in an OS Command ('OS Command Injection')24-Mar-2024 (S (OS)9.89.99.99.9 <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>						
Improper Neutralizat ion of Special Elements used in an OS Command (105 Command lnjection')24-Mar-20249.8A vulnerability classified as critical has been found in Tenda AC18 15.03.05.05. Affected is the function forth Efile goform/setsambaCon f of the file /goform/setsamba acfg. 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 sused. VDB- 257778 is the identifier assignedN/AO-TEN-AC18- 040424/117	Product: ac	18_firmware				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')24-Mar-20249.8classified as critical has been found in Tenda AC18 15.03.05.05. Affected is the function formSetSambaCon f of the file /goform/setsamb acfg. 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 assignedN/A0-TEN-AC18- 040424/117	Affected Ver	sion(s): 15.03.05	.05			
	Neutralizat ion of Special Elements used in an OS Command ('OS Command	24-Mar-2024	9.8	classified as critical has been found in Tenda AC18 15.03.05.05. Affected is the function formSetSambaCon f of the file /goform/setsamb acfg. 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	N/A	

Page **75** of **76**

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		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 76 of 76										