National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

01 - 15 Oct 2024 Vol. 11 No. 19

https://nciipc.gov.in/

Table of Content

Vendor	Product	Page Number
Apple	iphone_os	595
	macos	595
Cisco	meraki_mx100_firmware	598
	meraki_mx105_firmware	604
	meraki_mx250_firmware	610
	meraki_mx400_firmware	616
	meraki_mx450_firmware	622
	meraki_mx600_firmware	628
	meraki_mx64w_firmware	634
	meraki_mx64_firmware	640
	meraki_mx65w_firmware	646
	meraki_mx65_firmware	652
	meraki_mx67c_firmware	658
	meraki_mx67w_firmware	664
	meraki_mx67_firmware	670
	meraki_mx68cw_firmware	676
	meraki_mx68w_firmware	682
	meraki_mx68_firmware	688
	meraki_mx75_firmware	694
	meraki_mx84_firmware	700
	meraki_mx85_firmware	706
	meraki_mx95_firmware	712
	meraki_vmx_firmware	718
	meraki_z3c_firmware	724
	meraki_z3_firmware	730
	meraki_z4c_firmware	736
	meraki_z4_firmware	742
	rv042g_firmware	748
	rv042_firmware	988
	rv320_firmware	1228
	rv325_firmware	1467
	rv340w_dual_wan_gigabit_wireless-ac_vpn_router_firmware	1707

Vendor	Product	Page Number
Qualcomm	qca6595_firmware	1856
	qca6688aq_firmware	1856
	qca6696_firmware	1856
	qca6698aq_firmware	1856
	qcs410_firmware	1857
	qcs610_firmware	1857
	qcs6490_firmware	1857
	sa4150p_firmware	1857
	sa4155p_firmware	1857
	sa6145p_firmware	1858
	sa6150p_firmware	1858
	sa6155p_firmware	1858
	sa8145p_firmware	1858
	sa8150p_firmware	1858
	sa8155p_firmware	1859
	sa8195p_firmware	1859
	sa8295p_firmware	1859
	sd660_firmware	1859
	sd865_5g_firmware	1859
	sg4150p_firmware	1860
	snapdragon_660_mobile_firmware	1860
	snapdragon_680_4g_mobile_firmware	1860
	snapdragon_685_4g_mobile_firmware	1860
	snapdragon_865\+_5g_mobile_firmware	1860
	snapdragon_865_5g_mobile_firmware	1861
	snapdragon_870_5g_mobile_firmware	1861
	snapdragon_888\+_5g_mobile_firmware	1861
	snapdragon_888_5g_mobile_firmware	1861
	snapdragon_8_gen_1_mobile_firmware	1861
	snapdragon_auto_5g_modem-rf_firmware	1862
	snapdragon_auto_5g_modem-rf_gen_2_firmware	1862
	snapdragon_x55_5g_modem-rf_firmware	1862

Vendor	Product	Page Number
Qualcomm	snapdragon_xr2_5g_firmware	1862
	sw5100p_firmware	1862
	sw5100_firmware	1863
	sxr2130_firmware	1863
	video_collaboration_vc1_firmware	1863
	video_collaboration_vc3_firmware	1863
	wcd9335_firmware	1863
	wcd9341_firmware	1864
	wcd9370_firmware	1864
	wcd9375_firmware	1864
	wcd9380_firmware	1864
	wcd9385_firmware	1864
	wcn3950_firmware	1865
	wcn3980_firmware	1865
	wcn3988_firmware	1865
	wcn3990_firmware	1865
	wsa8810_firmware	1865
	wsa8815_firmware	1866
	wsa8830_firmware	1866
	wsa8835_firmware	1866

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: acekyd					
Product: display_medium_posts					
Affected Version(s): * Up to (including) 5.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	5.4	The Display Medium Posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's display_medium_posts shortcode in all versions up to, and including, 5.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-9445**	N/A	A-ACE-DISP-211024/1
Vendor: Adobe					
Product: animate					
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.8					
Access of Uninitialized Pointer	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47411**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/2
Out-of-bounds Write	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Stack-based	https://helpx.adobe.com/security/products/ani	A-ADO-ANIM-211024/3

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47410**	mate/apsb24-76.html	
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47412**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/4
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47413**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/5
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47414**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/6
Use After	09-Oct-2024	7.8	Animate versions 23.0.7,	https://helpx.ad	A-ADO-ANIM-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47415**	obe.com/security/products/animate/apsb24-76.html	211024/7
Integer Overflow or Wraparound	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47416**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/8
Out-of-bounds Write	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47417**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/9
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/10

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-47418		
Out-of-bounds Read	09-Oct-2024	5.5	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47419**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/11
Out-of-bounds Read	09-Oct-2024	5.5	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47420**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/12
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.5					
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47412**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/13
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could	https://helpx.adobe.com/security/products/animate/apsb24-	A-ADO-ANIM-211024/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47413**	76.html	
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47414**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/15
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47415**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/16
Integer Overflow or Wraparound	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47416**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/17
Out-of-bounds	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are	https://helpx.adobe.com/securit	A-ADO-ANIM-211024/18

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47417**	y/products/animate/apsb24-76.html	
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47418**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/19
Access of Uninitialized Pointer	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47411**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/20
Out-of-bounds Write	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/21

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-47410		
Out-of-bounds Read	09-Oct-2024	5.5	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47419**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/22
Out-of-bounds Read	09-Oct-2024	5.5	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47420**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	A-ADO-ANIM-211024/23
Product: commerce					
Affected Version(s): -					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/24

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/25
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/26
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**		
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/28
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/29
Improper Neutralization of Input During Web Page Generation ('Cross-site	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**		
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/31
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/32
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/34
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/35
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/37
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/38
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/40
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/41
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/43
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/44
Affected Version(s): 2.3.7					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/45

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this issue does not require user interaction. **CVE ID: CVE-2024-45115**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/46
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/47
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/48

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**		
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/49
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/50
Improper Neutralization of Input	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are	https://helpx.adobe.com/security/products/mag	A-ADO-COMM-211024/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	ento/apsb24-73.html	
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/52
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/53
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper	https://helpx.adobe.com/security/products/magento/apsb24-	A-ADO-COMM-211024/54

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	73.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/55
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/56
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/58
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/59
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/60

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/61
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/62
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/64
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/65
Affected Version(s): 2.4.0					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/66

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/67
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/68
N/A	10-Oct-2024	6.5	Adobe Commerce versions	https://helpx.ad	A-ADO-COMM-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	obe.com/security/products/magento/apsb24-73.html	211024/69
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/70
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45119		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/72
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/73
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45131		
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/75
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/76
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/77

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/78
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/79
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/80
N/A	10-Oct-2024	4.3	Adobe Commerce versions	https://helpx.ad	A-ADO-COMM-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	obe.com/security/products/magento/apsb24-73.html	211024/81
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/82
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/83

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/84
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/85
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/86
Affected Version(s): 2.4.1					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9,	https://helpx.adobe.com/securit	A-ADO-COMM-211024/87

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	y/products/magento/apsb24-73.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/88
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/89

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**		
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/90
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/91
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/93
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/94
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**		
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/96
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/97
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not require user interaction. **CVE ID: CVE-2024-45129**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/99
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/100
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction. **CVE ID: CVE-2024-45121**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/102
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/103
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/105
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/106
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45133		
Affected Version(s): 2.4.2					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/108
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/109
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**		
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/111
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/112
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/113

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/114
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/115
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**		
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/117
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/118
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**		
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/120
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/121
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/123
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/124
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/126
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/127
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/128

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**		
Affected Version(s): 2.4.3					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/129
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/130
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**		
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/132
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/133
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side	https://helpx.adobe.com/security/products/magento/apsb24-	A-ADO-COMM-211024/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	73.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/135
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/136
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are	https://helpx.adobe.com/security/products/mag	A-ADO-COMM-211024/137

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	ento/apsb24-73.html	
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/138
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/139
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are	https://helpx.adobe.com/security/products/mag	A-ADO-COMM-211024/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	ento/apsb24-73.html	
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/141
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/142
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/143

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/144
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/145
Time-of-check Time-of-use (TOCTOU) Race	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/146

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition			Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/147
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/148
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**		
Affected Version(s): 2.4.4					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/150
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/151
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are	https://helpx.adobe.com/security/products/mag	A-ADO-COMM-211024/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	ento/apsb24-73.html	
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/153
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/154

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/155
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/156
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/157

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45128		
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/158
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/159
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/160

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45127		
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/161
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/162
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/163

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/164
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/165
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/167
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/168
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/169
N/A	10-Oct-2024	2.7	Adobe Commerce versions	https://helpx.ad	A-ADO-COMM-

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	obe.com/security/products/magento/apsb24-73.html	211024/170
Affected Version(s): 2.4.5					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/171
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/172

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45116		
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/173
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/174
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**		
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/176
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/177
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**		
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/179
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/180
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**		
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/182
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/183
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this issue does not require user interaction. **CVE ID: CVE-2024-45122**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/185
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/186
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this issue does not require user interaction. **CVE ID: CVE-2024-45149**		
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/188
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/189
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user interaction. **CVE ID: CVE-2024-45135**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/191
Affected Version(s): 2.4.6					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/192
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**		
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/194
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/195
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/196

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**		
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/197
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/198
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**		
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/200
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/201
Improper Neutralization of Input During Web Page Generation ('Cross-site	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**		
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/203
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/204
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/206
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/207
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**		
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/209
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/210
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/211

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/212
Affected Version(s): 2.4.7					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/213
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**		
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/215
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/216
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are	https://helpx.adobe.com/security/products/mag	A-ADO-COMM-211024/217

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	ento/apsb24-73.html	
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/218
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/219
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper	https://helpx.adobe.com/security/products/magento/apsb24-	A-ADO-COMM-211024/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	73.html	
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/221
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/222
Improper Neutralization of Input	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are	https://helpx.adobe.com/security/products/mag	A-ADO-COMM-211024/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	ento/apsb24-73.html	
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/224
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/225
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/227
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/228
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**		
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/230
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/231
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/233
Product: commerce_b2b					
Affected Version(s): 1.3.3					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/234
Improper Neutralization of Input During Web Page	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS)	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**		
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/236
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/237

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45132		
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/238
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/239
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/240

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45123		
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/241
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/242
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction. **CVE ID: CVE-2024-45124**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/244
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/245
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45129		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/247
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/248
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/249

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45149		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/250
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/251
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/252

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45133		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/253
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/254
Affected Version(s): 1.3.4					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45115		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/256
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/257
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**		
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/259
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/260
Improper Neutralization of Input During Web Page	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS)	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**		
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/262
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/263
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/265
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/266
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/267

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/268
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/269
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/271
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/272
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/273

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/274
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/275
Affected Version(s): 1.3.5					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/277
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/278
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are	https://helpx.adobe.com/security/products/mag	A-ADO-COMM-211024/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	ento/apsb24-73.html	
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/280
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/281
Improper	10-Oct-2024	6.1	Adobe Commerce versions	https://helpx.ad	A-ADO-COMM-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	obe.com/security/products/magento/apsb24-73.html	211024/282
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/283
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/284
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9,	https://helpx.adobe.com/securit	A-ADO-COMM-211024/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	y/products/magento/apsb24-73.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/286
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/287
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper	https://helpx.adobe.com/security/products/magento/apsb24-	A-ADO-COMM-211024/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	73.html	
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/289
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/290
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/292
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/293
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information	https://helpx.adobe.com/security/products/magento/apsb24-	A-ADO-COMM-211024/294

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	73.html	
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/295
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/296
Affected Version(s): 1.4.2					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/297

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/298
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/299

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45117		
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/300
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/301
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user interaction and scope is changed. **CVE ID: CVE-2024-45119**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/303
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/304
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user interaction. **CVE ID: CVE-2024-45131**		
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/306
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/307
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/308

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45125		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/309
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/310
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45121		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/312
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/313
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requires user interaction. **CVE ID: CVE-2024-45120**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/315
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/316
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-COMM-211024/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: magento					
Affected Version(s): -					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/318
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/319
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**		
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/321
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/322
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/324
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/325
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**		
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/327
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/328
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/330
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/331
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/333
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/334
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/336
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/337
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**		
Affected Version(s): 2.4.3					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/339
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/340
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**		
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/342
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/343
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side	https://helpx.adobe.com/security/products/magento/apsb24-	A-ADO-MAGE-211024/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	73.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/345
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/346
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are	https://helpx.adobe.com/security/products/mag	A-ADO-MAGE-211024/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	ento/apsb24-73.html	
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/348
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/349
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are	https://helpx.adobe.com/security/products/mag	A-ADO-MAGE-211024/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	ento/apsb24-73.html	
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/351
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/352
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/354
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/355
Time-of-check Time-of-use (TOCTOU) Race	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/356

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition			Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/357
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/358
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**		
Affected Version(s): 2.4.4					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/360
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/361
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are	https://helpx.adobe.com/security/products/mag	A-ADO-MAGE-211024/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	ento/apsb24-73.html	
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/363
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/364

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/365
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/366
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45128		
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/368
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/369
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/370

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45127		
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/371
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/372
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/373

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/374
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/375
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/377
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/378
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/379
N/A	10-Oct-2024	2.7	Adobe Commerce versions	https://helpx.ad	A-ADO-MAGE-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	obe.com/security/products/magento/apsb24-73.html	211024/380
Affected Version(s): 2.4.5					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/381
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/382

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45116		
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/383
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/384
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity.	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**		
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/386
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/387
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**		
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/389
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/390
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**		
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/392
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/393
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not require user interaction. **CVE ID: CVE-2024-45129**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/395
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/396
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not require user interaction. **CVE ID: CVE-2024-45121**		
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/398
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/399
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction. **CVE ID: CVE-2024-45133**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/401
Affected Version(s): 2.4.6					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/402
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/403

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**		
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/404
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/405
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/406

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**		
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/407
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/408
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**		
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/410
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/411
Improper Neutralization of Input During Web Page Generation ('Cross-site	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**		
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/413
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/414
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**		
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/416
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/417
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**		
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/419
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/420
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/422
Affected Version(s): 2.4.7					
N/A	10-Oct-2024	9.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45115**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/423
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	8.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45116**		
N/A	10-Oct-2024	7.6	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45117**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/425
Incorrect Authorization	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45132**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/426
N/A	10-Oct-2024	6.5	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper	https://helpx.adobe.com/security/products/magento/apsb24-	A-ADO-MAGE-211024/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45118**	73.html	
Server-Side Request Forgery (SSRF)	10-Oct-2024	6.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed. **CVE ID: CVE-2024-45119**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/428
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-45123**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/429
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper	https://helpx.adobe.com/security/products/magento/apsb24-	A-ADO-MAGE-211024/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45128**	73.html	
Incorrect Authorization	10-Oct-2024	5.4	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45131**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/431
N/A	10-Oct-2024	5.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45124**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/432
Improper Neutralization of Input	10-Oct-2024	4.8	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are	https://helpx.adobe.com/security/products/mag	A-ADO-MAGE-211024/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-45127**	ento/apsb24-73.html	
Incorrect Authorization	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45125**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/434
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45130**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/435
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper	https://helpx.adobe.com/security/products/magento/apsb24-	A-ADO-MAGE-211024/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45129**	73.html	
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45122**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/437
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45121**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/438
N/A	10-Oct-2024	4.3	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/439

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45149**		
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2024	3.1	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction. **CVE ID: CVE-2024-45120**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/440
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45134**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/441
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/442

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45135**		
N/A	10-Oct-2024	2.7	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45133**	https://helpx.adobe.com/security/products/magento/apsb24-73.html	A-ADO-MAGE-211024/443
Vendor: andreamarinucci					
Product: notification_for_telegram					
Affected Version(s): * Up to (excluding) 3.3.2					
Missing Authorization	10-Oct-2024	4.3	The Notification for Telegram plugin for WordPress is vulnerable to unauthorized test message sending due to a missing capability check on the 'nftb_test_action' function in versions up to, and including, 3.3.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to send a test message via the Telegram Bot API to all users configured in the settings. **CVE ID: CVE-2024-9685**	https://plugins.trac.wordpress.org/changeset/3165615/notification-for-telegram	A-AND-NOTI-211024/444
Vendor: angeljudesuarez					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: placement_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2024	6.1	itsourcecode Placement Management System 1.0 is vulnerable to Cross Site Scripting (XSS) via the Full Name field in registration.php. **CVE ID: CVE-2024-46300**	N/A	A-ANG-PLAC-211024/445
Vendor: berqier					
Product: berqwp					
Affected Version(s): * Up to (excluding) 2.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-2024	6.1	The BerqWP – Automated All-In-One PageSpeed Optimization Plugin for Core Web Vitals, Cache, CDN, Images, CSS, and JavaScript plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'url' parameter in all versions up to, and including, 2.1.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9344**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3160806%40searchpro&new=3160806%40searchpro&sfp_email=&sfph_mail=	A-BER-BERQ-211024/446
Vendor: brevo					
Product: newsletter\,_smtp\,_email_marketing_and_subscribe					
Affected Version(s): * Up to (excluding) 3.1.88					
Cross-Site Request Forgery (CSRF)	10-Oct-2024	4.3	The Newsletter, SMTP, Email marketing and Subscribe forms by Brevo (formely Sendinblue) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up	https://plugins.trac.wordpress.org/changeset/3165451/mailin/tags/3.1.88/page/page-home.php	A-BRE-NEWS-211024/447

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to, and including, 3.1.87. This is due to missing or incorrect nonce validation on the Init() function. This makes it possible for unauthenticated attackers to log out of a Brevo connection via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-8477**		
Vendor: checkmk					
Product: checkmk					
Affected Version(s): 2.1.0					
Exposure of Sensitive Information to an Unauthorized Actor	10-Oct-2024	7.5	Information leakage in mknotifyd in Checkmk before 2.3.0p18, 2.2.0p36, 2.1.0p49 and in 2.0.0p39 (EOL) allows attacker to get potentially sensitive data **CVE ID: CVE-2024-6747**	https://checkmk.com/werk/17145	A-CHE-CHEC-211024/448
Affected Version(s): 2.2.0					
Exposure of Sensitive Information to an Unauthorized Actor	10-Oct-2024	7.5	Information leakage in mknotifyd in Checkmk before 2.3.0p18, 2.2.0p36, 2.1.0p49 and in 2.0.0p39 (EOL) allows attacker to get potentially sensitive data **CVE ID: CVE-2024-6747**	https://checkmk.com/werk/17145	A-CHE-CHEC-211024/449
Affected Version(s): 2.3.0					
Exposure of Sensitive Information to an Unauthorized Actor	10-Oct-2024	7.5	Information leakage in mknotifyd in Checkmk before 2.3.0p18, 2.2.0p36, 2.1.0p49 and in 2.0.0p39 (EOL) allows attacker to get potentially sensitive data **CVE ID: CVE-2024-6747**	https://checkmk.com/werk/17145	A-CHE-CHEC-211024/450
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.1.0					
Exposure of Sensitive Information	10-Oct-2024	7.5	Information leakage in mknotifyd in Checkmk before 2.3.0p18, 2.2.0p36,	https://checkmk.com/werk/17145	A-CHE-CHEC-211024/451

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to an Unauthorized Actor			2.1.0p49 and in 2.0.0p39 (EOL) allows attacker to get potentially sensitive data **CVE ID: CVE-2024-6747**		
Vendor: Cisco					
Product: identity_services_engine					
Affected Version(s): 2.7.0					
Missing Encryption of Sensitive Data	02-Oct-2024	6.5	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to a lack of proper data protection mechanisms for certain configuration settings. An attacker with Read-Only Administrator privileges could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to view device credentials that are normally not visible to Read-Only Administrators. **CVE ID: CVE-2024-20515**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-disc-ZYF2nEEX	A-CIS-IDEN-211024/452
Affected Version(s): 3.0.0					
Missing Encryption of Sensitive Data	02-Oct-2024	6.5	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-disc-ZYF2nEEX	A-CIS-IDEN-211024/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lack of proper data protection mechanisms for certain configuration settings. An attacker with Read-Only Administrator privileges could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to view device credentials that are normally not visible to Read-Only Administrators. **CVE ID: CVE-2024-20515**		
Affected Version(s): 3.1.0					
Missing Encryption of Sensitive Data	02-Oct-2024	6.5	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to a lack of proper data protection mechanisms for certain configuration settings. An attacker with Read-Only Administrator privileges could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to view device credentials that are normally not visible to Read-Only Administrators. **CVE ID: CVE-2024-20515**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-disc-ZYF2nEEX	A-CIS-IDEN-211024/454
Affected Version(s): 3.2.0					
Missing Encryption of Sensitive Data	02-Oct-2024	6.5	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	A-CIS-IDEN-211024/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to a lack of proper data protection mechanisms for certain configuration settings. An attacker with Read-Only Administrator privileges could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to view device credentials that are normally not visible to Read-Only Administrators. **CVE ID: CVE-2024-20515**	ecurityAdvisory/cisco-sa-ise-info-disc-ZYF2nEEX	
Affected Version(s): 3.3.0					
Missing Encryption of Sensitive Data	02-Oct-2024	6.5	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to a lack of proper data protection mechanisms for certain configuration settings. An attacker with Read-Only Administrator privileges could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to view device credentials that are normally not visible to Read-Only Administrators.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-disc-ZYF2nEEX	A-CIS-IDEN-211024/456

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20515		
Affected Version(s): 3.4.0					
Missing Encryption of Sensitive Data	02-Oct-2024	6.5	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to a lack of proper data protection mechanisms for certain configuration settings. An attacker with Read-Only Administrator privileges could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to view device credentials that are normally not visible to Read-Only Administrators. **CVE ID: CVE-2024-20515**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-disc-ZYF2nEEX	A-CIS-IDEN-211024/457
Product: nexus_dashboard					
Affected Version(s): * Up to (excluding) 3.2\(1e\)					
N/A	02-Oct-2024	6.5	A vulnerability in a specific REST API endpoint of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to learn sensitive information on an affected device. This vulnerability is due to insufficient authorization controls on the affected REST API endpoint. An attacker could exploit this vulnerability by sending	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-uaapi-Jh4V6zpN	A-CIS-NEXU-211024/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted API requests to the affected endpoint. A successful exploit could allow the attacker to download config only or full backup files and learn sensitive configuration information. This vulnerability only affects a specific REST API endpoint and does not affect the web-based management interface. **CVE ID: CVE-2024-20441**		
Missing Authorization	02-Oct-2024	5.4	A vulnerability in the REST API endpoints of Cisco Nexus Dashboard could allow an authenticated, low-privileged, remote attacker to perform limited Administrator actions on an affected device. This vulnerability is due to insufficient authorization controls on some REST API endpoints. An attacker could exploit this vulnerability by sending crafted API requests to an affected endpoint. A successful exploit could allow the attacker to perform limited Administrator functions such as viewing portions of the web UI, generating config only or full backup files, and deleting tech support files. This vulnerability only affects a subset of REST API endpoints and does not affect the web-based management interface. **CVE ID: CVE-2024-20442**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-uaapi-Jh4V6zpN	A-CIS-NEXU-211024/459
Missing	02-Oct-2024	5.4	A vulnerability in a specific	https://sec.clou	A-CIS-NEXU-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization			REST API endpoint of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to upload or delete files on an affected device. This vulnerability exists because of missing authorization controls on the affected REST API endpoint. An attacker could exploit this vulnerability by sending crafted API requests to the affected endpoint. A successful exploit could allow the attacker to upload files into a specific container or delete files from a specific folder within that container. This vulnerability only affects a specific REST API endpoint and does not affect the web-based management interface. **CVE ID: CVE-2024-20477**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-uaapi-Jh4V6zpN	211024/460
Missing Authorization	02-Oct-2024	5.4	A vulnerability in the REST API endpoints of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to read or write files on an affected device. This vulnerability exists because of missing authorization controls on some REST API endpoints. An attacker could exploit this vulnerability by sending crafted API requests to an affected endpoint. A successful exploit could allow the attacker to perform limited	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-uaapi-Jh4V6zpN	A-CIS-NEXU-211024/461

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network-admin functions such as reading device configuration information, uploading files, and modifying uploaded files. Note: This vulnerability only affects a subset of REST API endpoints and does not affect the web-based management interface. **CVE ID: CVE-2024-20438**		
Product: nexus_dashboard_fabric_controller					
Affected Version(s): * Up to (excluding) 12.2.2					
Cleartext Storage of Sensitive Information	02-Oct-2024	8.6	A vulnerability in the Cisco Nexus Dashboard Fabric Controller (NDFC) software, formerly Cisco Data Center Network Manager (DCNM), could allow an attacker with access to a backup file to view sensitive information. This vulnerability is due to the improper storage of sensitive information within config only and full backup files. An attacker could exploit this vulnerability by parsing the contents of a backup file that is generated from an affected device. A successful exploit could allow the attacker to access sensitive information, including NDFC-connected device credentials, the NDFC site manager private key, and the scheduled backup file encryption key. **CVE ID: CVE-2024-20448**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-cidv-XvyX2wLj	A-CIS-NEXU-211024/462
Improper Neutralization of	02-Oct-2024	5.5	A vulnerability in Cisco Nexus Dashboard Fabric Controller (NDFC), formerly	https://sec.cloudapps.cisco.com/security/center	A-CIS-NEXU-211024/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Argument Delimiters in a Command ('Argument Injection')			Cisco Data Center Network Manager (DCNM), could allow an authenticated, remote attacker with network-admin privileges to perform a command injection attack against an affected device. This vulnerability is due to insufficient validation of command arguments. An attacker could exploit this vulnerability by submitting crafted command arguments to a specific REST API endpoint. A successful exploit could allow the attacker to overwrite sensitive files or crash a specific container, which would restart on its own, causing a low-impact denial of service (DoS) condition. **CVE ID: CVE-2024-20444**	/content/CiscoSecurityAdvisory/cisco-sa-ndfc-raci-T46k3jnN	
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.2.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	8.8	A vulnerability in the REST API and web UI of Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, low-privileged, remote attacker to perform a command injection attack against an affected device. This vulnerability is due to improper user authorization and insufficient validation of command arguments. An attacker could exploit this vulnerability by submitting crafted commands to an affected REST API endpoint	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-cmdinj-UvYZrKfr	A-CIS-NEXU-211024/464

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or through the web UI. A successful exploit could allow the attacker to execute arbitrary commands on the CLI of a Cisco NDFC-managed device with network-admin privileges. Note: This vulnerability does not affect Cisco NDFC when it is configured for storage area network (SAN) controller deployment. **CVE ID: CVE-2024-20432**		
N/A	02-Oct-2024	6.5	A vulnerability in a specific REST API endpoint of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to learn sensitive information on an affected device. This vulnerability is due to insufficient authorization controls on the affected REST API endpoint. An attacker could exploit this vulnerability by sending crafted API requests to the affected endpoint. A successful exploit could allow the attacker to download config only or full backup files and learn sensitive configuration information. This vulnerability only affects a specific REST API endpoint and does not affect the web-based management interface. **CVE ID: CVE-2024-20441**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-uaapi-Jh4V6zpN	A-CIS-NEXU-211024/465
Missing	02-Oct-2024	5.4	A vulnerability in a specific	https://sec.clou	A-CIS-NEXU-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization			REST API endpoint of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to upload or delete files on an affected device. This vulnerability exists because of missing authorization controls on the affected REST API endpoint. An attacker could exploit this vulnerability by sending crafted API requests to the affected endpoint. A successful exploit could allow the attacker to upload files into a specific container or delete files from a specific folder within that container. This vulnerability only affects a specific REST API endpoint and does not affect the web-based management interface. **CVE ID: CVE-2024-20477**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-uaapi-Jh4V6zpN	211024/466
Missing Authorization	02-Oct-2024	5.4	A vulnerability in the REST API endpoints of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to read or write files on an affected device. This vulnerability exists because of missing authorization controls on some REST API endpoints. An attacker could exploit this vulnerability by sending crafted API requests to an affected endpoint. A successful exploit could allow the attacker to perform limited	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-uaapi-Jh4V6zpN	A-CIS-NEXU-211024/467

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network-admin functions such as reading device configuration information, uploading files, and modifying uploaded files. Note: This vulnerability only affects a subset of REST API endpoints and does not affect the web-based management interface. **CVE ID: CVE-2024-20438**		
Affected Version(s): From (including) 12.0.0 Up to (including) 12.2.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Oct-2024	8.8	A vulnerability in Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, remote attacker with low privileges to execute arbitrary code on an affected device. This vulnerability is due to improper path validation. An attacker could exploit this vulnerability by using the Secure Copy Protocol (SCP) to upload malicious code to an affected device using path traversal techniques. A successful exploit could allow the attacker to execute arbitrary code in a specific container with the privileges of root. **CVE ID: CVE-2024-20449**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-ptrce-BUSHLbp	A-CIS-NEXU-211024/468
Missing Authorization	02-Oct-2024	5.4	A vulnerability in the REST API endpoints of Cisco Nexus Dashboard could allow an authenticated, low-privileged, remote attacker to perform limited Administrator actions on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-uaapi-Jh4V6zpN	A-CIS-NEXU-211024/469

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient authorization controls on some REST API endpoints. An attacker could exploit this vulnerability by sending crafted API requests to an affected endpoint. A successful exploit could allow the attacker to perform limited Administrator functions such as viewing portions of the web UI, generating config only or full backup files, and deleting tech support files. This vulnerability only affects a subset of REST API endpoints and does not affect the web-based management interface. **CVE ID: CVE-2024-20442**		
Affected Version(s): From (including) 12.1.0 Up to (excluding) 12.2.2.241					
Insertion of Sensitive Information into Log File	02-Oct-2024	8.6	A vulnerability in a logging function of Cisco Nexus Dashboard Insights could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because remote controller credentials are recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view remote controller admin credentials in clear text.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-idv-Bk8VqEDc	A-CIS-NEXU-211024/470

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information. **CVE ID: CVE-2024-20491**		
Insertion of Sensitive Information into Log File	02-Oct-2024	8.6	A vulnerability in a logging function of Cisco Nexus Dashboard Fabric Controller (NDFC) and Cisco Nexus Dashboard Orchestrator (NDO) could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because HTTP proxy credentials could be recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view HTTP proxy server admin credentials in clear text that are configured on Nexus Dashboard to reach an external network. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information. **CVE ID: CVE-2024-20490**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-idv-Bk8VqEDc	A-CIS-NEXU-211024/471
Product: nexus_dashboard_insights					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 6.4.0					
Insertion of Sensitive Information into Log File	02-Oct-2024	8.6	A vulnerability in a logging function of Cisco Nexus Dashboard Insights could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because remote controller credentials are recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view remote controller admin credentials in clear text. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information. **CVE ID: CVE-2024-20491**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-idv-Bk8VqEDc	A-CIS-NEXU-211024/472
Insertion of Sensitive Information into Log File	02-Oct-2024	8.6	A vulnerability in a logging function of Cisco Nexus Dashboard Fabric Controller (NDFC) and Cisco Nexus Dashboard Orchestrator (NDO) could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because HTTP proxy credentials could be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-idv-Bk8VqEDc	A-CIS-NEXU-211024/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view HTTP proxy server admin credentials in clear text that are configured on Nexus Dashboard to reach an external network. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information. **CVE ID: CVE-2024-20490**		
Affected Version(s): From (including) 6.5.0 Up to (excluding) 6.5.1.32					
Insertion of Sensitive Information into Log File	02-Oct-2024	8.6	A vulnerability in a logging function of Cisco Nexus Dashboard Insights could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because remote controller credentials are recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view remote controller admin credentials in clear text. Note: Best practice is to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-idv-Bk8VqEDc	A-CIS-NEXU-211024/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information. **CVE ID: CVE-2024-20491**		
Insertion of Sensitive Information into Log File	02-Oct-2024	8.6	A vulnerability in a logging function of Cisco Nexus Dashboard Fabric Controller (NDFC) and Cisco Nexus Dashboard Orchestrator (NDO) could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because HTTP proxy credentials could be recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view HTTP proxy server admin credentials in clear text that are configured on Nexus Dashboard to reach an external network. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information. **CVE ID: CVE-2024-20490**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-idv-Bk8VqEDc	A-CIS-NEXU-211024/475
Product: nexus_dashboard_orchestrator					
Affected Version(s): * Up to (excluding) 4.2\(3o\)					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	02-Oct-2024	8.6	A vulnerability in a logging function of Cisco Nexus Dashboard Insights could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because remote controller credentials are recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view remote controller admin credentials in clear text. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information. **CVE ID: CVE-2024-20491**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-idv-Bk8VqEDc	A-CIS-NEXU-211024/476
Insertion of Sensitive Information into Log File	02-Oct-2024	8.6	A vulnerability in a logging function of Cisco Nexus Dashboard Fabric Controller (NDFC) and Cisco Nexus Dashboard Orchestrator (NDO) could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because HTTP proxy credentials could be recorded in an internal log	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-idv-Bk8VqEDc	A-CIS-NEXU-211024/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view HTTP proxy server admin credentials in clear text that are configured on Nexus Dashboard to reach an external network. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information. **CVE ID: CVE-2024-20490**		
Improper Certificate Validation	02-Oct-2024	5.9	A vulnerability in the SSL/TLS implementation of Cisco Nexus Dashboard Orchestrator (NDO) could allow an unauthenticated, remote attacker to intercept sensitive information from an affected device. This vulnerability exists because the Cisco NDO Validate Peer Certificate site management feature validates the certificates for Cisco Application Policy Infrastructure Controller (APIC), Cisco Cloud Network Controller (CNC), and Cisco Nexus Dashboard only when a new site is added or an existing one is reregistered. An attacker could exploit this vulnerability by using machine-in-the-middle techniques to intercept the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndo-tlsvld-FdUF3cpw	A-CIS-NEXU-211024/478

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic between the affected device and Cisco NDO and then using a crafted certificate to impersonate the affected device. A successful exploit could allow the attacker to learn sensitive information during communications between these devices. **CVE ID: CVE-2024-20385**		
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.4\(1.1009\)					
Improper Certificate Validation	02-Oct-2024	5.9	A vulnerability in the SSL/TLS implementation of Cisco Nexus Dashboard Orchestrator (NDO) could allow an unauthenticated, remote attacker to intercept sensitive information from an affected device. This vulnerability exists because the Cisco NDO Validate Peer Certificate site management feature validates the certificates for Cisco Application Policy Infrastructure Controller (APIC), Cisco Cloud Network Controller (CNC), and Cisco Nexus Dashboard only when a new site is added or an existing one is reregistered. An attacker could exploit this vulnerability by using machine-in-the-middle techniques to intercept the traffic between the affected device and Cisco NDO and then using a crafted certificate to impersonate the affected device. A successful exploit could allow the attacker to learn sensitive information during communications between these devices.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndo-tlsvld-FdUF3cpw	A-CIS-NEXU-211024/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20385		
Affected Version(s): From (including) 4.4.0 Up to (excluding) 4.4.1.1012					
Insertion of Sensitive Information into Log File	02-Oct-2024	8.6	A vulnerability in a logging function of Cisco Nexus Dashboard Insights could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because remote controller credentials are recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view remote controller admin credentials in clear text. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information. **CVE ID: CVE-2024-20491**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-idv-Bk8VqEDc	A-CIS-NEXU-211024/480
Insertion of Sensitive Information into Log File	02-Oct-2024	8.6	A vulnerability in a logging function of Cisco Nexus Dashboard Fabric Controller (NDFC) and Cisco Nexus Dashboard Orchestrator (NDO) could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-idv-Bk8VqEDc	A-CIS-NEXU-211024/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because HTTP proxy credentials could be recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view HTTP proxy server admin credentials in clear text that are configured on Nexus Dashboard to reach an external network. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information. **CVE ID: CVE-2024-20490**		
Product: telepresence_video_communication_server					
Affected Version(s): x12.5.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x12.5.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x12.5.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20492		
Affected Version(s): x12.5.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/485
Affected Version(s): x12.5.4					
Improper Neutralization of Special Elements used in a	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	A-CIS-TELE-211024/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	/cisco-sa-expw-escalation-3bkz77bD	
Affected Version(s): x12.5.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x12.5.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x12.5.7					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/489

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x12.5.8					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/490

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): x12.5.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/491
Affected Version(s): x12.6.0					
Improper Neutralization of Special Elements used in a Command ('Command	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-	A-CIS-TELE-211024/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Injection')			system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	3bkz77bD	
Affected Version(s): x12.6.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/493

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x12.6.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x12.6.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/495

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x12.6.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/496
Affected Version(s): x12.7.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/497
Affected Version(s): x12.7.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.0.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.0.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.0.10					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.0.11					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/502
Affected Version(s): x14.0.2					
Improper Neutralizati	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco	https://sec.cloudapps.cisco.com	A-CIS-TELE-211024/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Special Elements used in a Command ('Command Injection')			Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	
Affected Version(s): x14.0.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.0.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/505

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.0.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.0.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/507

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.0.7					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/508
Affected Version(s): x14.0.8					
Improper Neutralization of Special Elements	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	A-CIS-TELE-211024/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	ecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	
Affected Version(s): x14.0.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.2.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.2.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20492		
Affected Version(s): x14.2.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/514
Affected Version(s): x14.2.6					
Improper Neutralization of Special Elements used in a	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	A-CIS-TELE-211024/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	/cisco-sa-expw-escalation-3bkz77bD	
Affected Version(s): x14.2.7					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.3.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.3.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.3.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/519

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): x14.3.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/520
Affected Version(s): x14.3.4					
Improper Neutralization of Special Elements used in a Command ('Command	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-	A-CIS-TELE-211024/521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Injection')			system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	3bkz77bD	
Affected Version(s): x14.3.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/522

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x14.3.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x15.0.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/524

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x15.0.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/525
Affected Version(s): x15.0.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/526
Affected Version(s): x15.0.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/528

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.1.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.10.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/531
Affected Version(s): x8.10.1					
Improper Neutralizati	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco	https://sec.cloudapps.cisco.com	A-CIS-TELE-211024/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Special Elements used in a Command ('Command Injection')			Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	
Affected Version(s): x8.10.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.10.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.10.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.11.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.11.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/537
Affected Version(s): x8.11.2					
Improper Neutralization of Special Elements	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	A-CIS-TELE-211024/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	ecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	
Affected Version(s): x8.11.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.11.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.2.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20492		
Affected Version(s): x8.2.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/543
Affected Version(s): x8.5					
Improper Neutralization of Special Elements used in a	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	A-CIS-TELE-211024/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	/cisco-sa-expw-escalation-3bkz77bD	
Affected Version(s): x8.5.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.5.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.5.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/547

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/548

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): x8.6.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/549
Affected Version(s): x8.7					
Improper Neutralization of Special Elements used in a Command ('Command	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-	A-CIS-TELE-211024/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Injection')			system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	3bkz77bD	
Affected Version(s): x8.7.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/551

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.7.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.7.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.8					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/554
Affected Version(s): x8.8.1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/555
Affected Version(s): x8.8.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.8.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.9.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**		
Affected Version(s): x8.9.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	6.7	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. **CVE ID: CVE-2024-20492**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD	A-CIS-TELE-211024/560
Product: unified_computing_system					
Affected Version(s): 4.1\(2a\)					
Improper	02-Oct-2024	7.2	A vulnerability in the	https://sec.clou	A-CIS-UNIF-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	211024/561
Affected Version(s): 4.1\(2b\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.1\(2c\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/563
Affected Version(s): 4.1\(3a\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.1\(3b\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/565
Affected Version(s): 4.1\(3c\)					
Improper Neutralizati	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-	https://sec.cloudapps.cisco.com	A-CIS-UNIF-211024/566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Special Elements used in a Command ('Command Injection')			Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	
Affected Version(s): 4.1\(3d\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.1\(3e\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/568
Affected Version(s): 4.1\(3f\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.1\(3h\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/570
Affected Version(s): 4.1\(3i\)					
Improper Neutralization of Special	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed	https://sec.cloudapps.cisco.com/security/center	A-CIS-UNIF-211024/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	
Affected Version(s): 4.1\(3j\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.1\(3k\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/573
Affected Version(s): 4.1\(3l\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.1\(3m\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/575
Affected Version(s): 4.1\(4a\)					
Improper Neutralization of Special Elements	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	A-CIS-UNIF-211024/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	ecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	
Affected Version(s): 4.2\(1c\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.2\(1d\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/578
Affected Version(s): 4.2\(1f\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.2\(1i\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/580
Affected Version(s): 4.2\(1k\)					
Improper Neutralization of Special Elements used in a	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	A-CIS-UNIF-211024/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	
Affected Version(s): 4.2\(1l\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.2\(1m\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/583
Affected Version(s): 4.2\(1n\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.2\(2a\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/585
Affected Version(s): 4.2\(2c\)					
Improper Neutralization of Special Elements used in a Command	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-	A-CIS-UNIF-211024/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	redfish-cominj-sbkv5ZZ	
Affected Version(s): 4.2\(2d\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20365		
Affected Version(s): 4.2\(2e\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/588
Affected Version(s): 4.2\(3b\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.2\(3d\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/590
Affected Version(s): 4.2\(3e\)					
Improper Neutralization of Special Elements used in a Command ('Command	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-	A-CIS-UNIF-211024/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Injection')			administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	sbkv5ZZ	
Affected Version(s): 4.2\(3g\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20365		
Affected Version(s): 4.2\(3h\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/593
Affected Version(s): 4.2\(3i\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.2\(3j\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/595
Affected Version(s): 4.2\(3k\)					
Improper Neutralization of Special Elements used in a Command ('Command	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-	A-CIS-UNIF-211024/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Injection')			administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	sbkv5ZZ	
Affected Version(s): 4.3\(2b\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20365		
Affected Version(s): 4.3\(2c\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/598
Affected Version(s): 4.3\(2e\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**		
Affected Version(s): 4.3\(3a\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/600
Affected Version(s): 4.3\(3c\)					
Improper Neutralization of Special Elements used in a Command ('Command	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-	A-CIS-UNIF-211024/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Injection')			administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	sbkv5ZZ	
Affected Version(s): 4.3\(4a\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20365		
Affected Version(s): 4.3\(4b\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Oct-2024	7.2	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID: CVE-2024-20365**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ	A-CIS-UNIF-211024/603
Vendor: clio					
Product: clio_grow					
Affected Version(s): * Up to (including) 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	The Clio Grow plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.0.2. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an	N/A	A-CLI-CLIO-211024/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action such as clicking on a link. **CVE ID: CVE-2024-8802**		
Vendor: code-projects					
Product: blood_bank_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Oct-2024	7.5	A vulnerability, which was classified as critical, was found in code-projects Blood Bank System 1.0. Affected is an unknown function of the file register.php. The manipulation of the argument user leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9797**	N/A	A-COD-BLOO-211024/605
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	5.4	A vulnerability was found in code-projects Blood Bank System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/campsdetails.php. The manipulation of the argument hospital/address/city/contact leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "hospital". **CVE ID: CVE-2024-9805**	N/A	A-COD-BLOO-211024/606
Improper Neutralization of Special Elements used in an SQL	10-Oct-2024	4.9	A vulnerability was found in code-projects Blood Bank System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file	N/A	A-COD-BLOO-211024/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			/admin/campsdetails.php. The manipulation of the argument hospital leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. **CVE ID: CVE-2024-9804**		
Product: crud_operation_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Oct-2024	9.8	A vulnerability classified as critical was found in code-projects Crud Operation System 1.0. This vulnerability affects unknown code of the file delete.php. The manipulation of the argument sid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9812**	N/A	A-COD-CRUD-211024/608
Product: restaurant_reservation_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Oct-2024	9.8	A vulnerability classified as critical has been found in code-projects Restaurant Reservation System 1.0. This affects an unknown part of the file filter3.php. The manipulation of the argument company leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9811**	N/A	A-COD-REST-211024/609
Improper Neutralization of Special	02-Oct-2024	9.8	A vulnerability has been found in code-projects Restaurant Reservation	N/A	A-COD-REST-211024/610

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /filter2.php. The manipulation of the argument from/to leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "from" to be affected. But it must be assumed that parameter "to" is affected as well. **CVE ID: CVE-2024-9429**		
Vendor: coderevolution					
Product: echo_rss_feed_post_generator					
Affected Version(s): * Up to (excluding) 5.4.7					
N/A	01-Oct-2024	9.8	The Echo RSS Feed Post Generator plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 5.4.6. This is due to the plugin not properly restricting the roles that can set during registration through the echo_check_post_header_sent() function. This makes it possible for unauthenticated attackers to register as an administrator. **CVE ID: CVE-2024-9265**	N/A	A-COD-ECHO-211024/611
Vendor: codezips					
Product: online_shopping_portal					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	10-Oct-2024	9.8	A vulnerability, which was classified as critical, has been found in Codezips Online Shopping Portal 1.0. This issue affects some	N/A	A-COD-ONLI-211024/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unknown processing of the file /update-image1.php. The manipulation of the argument productimage1 leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9794**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Oct-2024	9.8	A vulnerability was found in Codezips Online Shopping Portal 1.0. It has been classified as critical. Affected is an unknown function of the file index.php. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9460**	N/A	A-COD-ONLI-211024/613
Product: pharmacy_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Oct-2024	9.8	A vulnerability, which was classified as critical, has been found in Codezips Pharmacy Management System 1.0. This issue affects some unknown processing of the file product/register.php. The manipulation of the argument category leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9813**	N/A	A-COD-PHAR-211024/614
Vendor: connekthq					
Product: ajax_load_more					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 7.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-2024	5.4	The WordPress Infinite Scroll – Ajax Load More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button_label' parameter in all versions up to, and including, 7.1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-8505**	https://plugins.trac.wordpress.org/changeset/3160896/	A-CON-AJAX-211024/615
Vendor: contempo					
Product: pdf_image_generator					
Affected Version(s): * Up to (including) 1.5.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-2024	6.1	The PDF Image Generator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.5.6. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9241**	N/A	A-CON-PDF_-211024/616
Vendor: cornelraiu					
Product: wp_search_analytics					
Affected Version(s): * Up to (excluding) 1.4.11					
Improper	01-Oct-2024	6.1	The WP Search Analytics	N/A	A-COR-WP_S-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.4.10. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9209**		211024/617
Vendor: cozmoslabs					
Product: membership_\&_content_restriction_-_paid_member_subscriptions					
Affected Version(s): * Up to (excluding) 2.12.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-2024	6.1	The Paid Membership Subscriptions – Effortless Memberships, Recurring Payments & Content Restriction plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.12.8. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9222**	https://plugins.trac.wordpress.org/changeset/3160323/#file10	A-COZ-MEMB-211024/618
Vendor: cssjockey					
Product: wp_builder					
Affected Version(s): * Up to (including) 3.0.7					
Improper Neutralizati	10-Oct-2024	5.4	The WP Builder plugin for WordPress is vulnerable to	N/A	A-CSS-WP_B-211024/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 3.0.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. **CVE ID: CVE-2024-9457**		
Vendor: curator					
Product: curator.io					
Affected Version(s): * Up to (including) 1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	5.4	The Curator.io: Show all your social media posts in a beautiful feed. plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'feed_id' attribute in all versions up to, and including, 1.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-9057**	N/A	A-CUR-CURA-211024/620
Vendor: davidartiss					
Product: code_embed					
Affected Version(s): * Up to (excluding) 2.5					
Improper Neutralization of Input During Web Page Generation	04-Oct-2024	5.4	The Code Embed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's script embed functionality in all versions up to, and	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=316221	A-DAV-CODE-211024/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			including, 2.4 due to insufficient restrictions on who can utilize the functionality. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-8804**	9%40simple-embed-code&new=3162219%40simple-embed-code&sfp_email=&sfph_mail=	
Vendor: definetlynotai					
Product: logicytics					
Affected Version(s): * Up to (including) 2.3.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Oct-2024	9.8	Logicytics is designed to harvest and collect data for forensic analysis. Logicytics has a basic vuln affecting compromised devices from shell injections. This vulnerability is fixed in 2.3.2. **CVE ID: CVE-2024-47608**	https://github.com/DefinetlyNotAI/Logicytics/security/advisories/GHSA-5wvr-vvqf-668m	A-DEF-LOGI-211024/622
Vendor: deltaww					
Product: diaenergie					
Affected Version(s): * Up to (including) 1.10.01.008					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Oct-2024	9.8	Delta Electronics DIAEnergie is vulnerable to an SQL injection in the script AM_RegReport.aspx. An unauthenticated attacker may be able to exploit this issue to obtain records contained in the targeted product. **CVE ID: CVE-2024-43699**	https://www.deltaww.com/en-US/Cybersecurity_Advisory	A-DEL-DIAE-211024/623
Improper Neutralization of Special Elements used in an SQL Command ('SQL	03-Oct-2024	8.8	Delta Electronics DIAEnergie is vulnerable to an SQL injection in the script Handler_CFG.ashx. An authenticated attacker may be able to exploit this issue to cause delay in the targeted product.	https://www.deltaww.com/en-US/Cybersecurity_Advisory	A-DEL-DIAE-211024/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Injection')			**CVE ID: CVE-2024-42417**		
Vendor: duckdev					
Product: loggedin					
Affected Version(s): * Up to (excluding) 1.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-2024	6.1	The Loggedin – Limit Active Logins plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.3.1. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This is only exploitable when the leave a review notice is present. **CVE ID: CVE-2024-9228**	N/A	A-DUC-LOGG-211024/625
Vendor: emiloimagtolis					
Product: online_discussion_forum					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	04-Oct-2024	8.8	File Upload vulnerability in Itsourcecode Online Discussion Forum Project v.1.0 allows a remote attacker to execute arbitrary code via the "sendreply.php" file, and the uploaded file was received using the "$- FILES" variable. **CVE ID: CVE-2024-37868**	N/A	A-EMI-ONLI-211024/626
Unrestricted Upload of File with Dangerous Type	04-Oct-2024	8.8	File Upload vulnerability in Itsourcecode Online Discussion Forum Project v.1.0 allows a remote attacker to execute arbitrary code via the "poster.php" file, and the	N/A	A-EMI-ONLI-211024/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uploaded file was received using the "$- FILES" variable **CVE ID: CVE-2024-37869**		
Vendor: esafenet					
Product: cdg					
Affected Version(s): v5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-2024	8.8	A vulnerability was found in ESAFENET CDG V5. It has been rated as critical. Affected by this issue is the function delCatelogs of the file /CDGServer3/document/Catelogs;logindojojs?command=DelCatelogs. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9560**	N/A	A-ESA-CDG-211024/628
Vendor: Esri					
Product: portal_for_arcgis					
Affected Version(s): * Up to (including) 11.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	5.4	There is an HTML injection vulnerability in Esri Portal for ArcGIS versions 11.0 and below that may allow a remote, authenticated attacker to create a crafted link which when clicked could render arbitrary HTML in the victim's browser (no stateful change made or customer data rendered). **CVE ID: CVE-2024-38039**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	A-ESR-PORT-211024/629
Affected Version(s): * Up to (including) 11.1					
Improper Neutralization of Input	04-Oct-2024	4.8	There is a reflected cross site scripting in Esri Portal for ArcGIS 11.1 and below	https://www.esri.com/arcgis-blog/products/t	A-ESR-PORT-211024/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			on Windows and Linux x64 allows a remote authenticated attacker with administrative access to supply a crafted string which could potentially execute arbitrary JavaScript code in the their own browser (Self XSS). A user cannot be phished into clicking a link to execute code. **CVE ID: CVE-2024-25707**	rust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	
Affected Version(s): 10.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID: CVE-2024-38038**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	A-ESR-PORT-211024/631
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	5.4	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID: CVE-2024-38036**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	A-ESR-PORT-211024/632
Affected Version(s): 10.8.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-	A-ESR-PORT-211024/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID: CVE-2024-38038**	update-2-released/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 11.1, 10.9.1 and 10.8.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID: CVE-2024-25691**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	A-ESR-PORT-211024/634
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	5.4	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID: CVE-2024-38036**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	A-ESR-PORT-211024/635
Affected Version(s): 10.9.1					
N/A	04-Oct-2024	7.5	There is a local file inclusion vulnerability in Esri Portal for ArcGIS 11.2. 11.1, 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a URL that could potentially disclose sensitive configuration information by reading internal files. **CVE ID: CVE-2024-38040**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	A-ESR-PORT-211024/636
URL Redirection to Untrusted Site ('Open Redirect')	04-Oct-2024	6.1	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a URL that	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-	A-ESR-PORT-211024/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could redirect a victim to an arbitrary website, simplifying phishing attacks. **CVE ID: CVE-2024-38037**	for-arcgis-security-2024-update-2-released/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID: CVE-2024-38038**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	A-ESR-PORT-211024/638
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 11.1, 10.9.1 and 10.8.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID: CVE-2024-25691**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	A-ESR-PORT-211024/639
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	5.4	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID: CVE-2024-38036**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	A-ESR-PORT-211024/640
Affected Version(s): 11.0					
N/A	04-Oct-2024	7.5	There is a local file inclusion vulnerability in Esri Portal for ArcGIS 11.2. 11.1, 11.0 and 10.9.1 that may allow a	https://www.esri.com/arcgis-blog/products/trust-	A-ESR-PORT-211024/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote, unauthenticated attacker to craft a URL that could potentially disclose sensitive configuration information by reading internal files. **CVE ID: CVE-2024-38040**	arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	
URL Redirection to Untrusted Site ('Open Redirect')	04-Oct-2024	6.1	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks. **CVE ID: CVE-2024-38037**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	A-ESR-PORT-211024/642
Affected Version(s): 11.1					
N/A	04-Oct-2024	7.5	There is a local file inclusion vulnerability in Esri Portal for ArcGIS 11.2. 11.1, 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a URL that could potentially disclose sensitive configuration information by reading internal files. **CVE ID: CVE-2024-38040**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	A-ESR-PORT-211024/643
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 11.1, 10.9.1 and 10.8.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID: CVE-2024-25691**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	A-ESR-PORT-211024/644
Affected Version(s): 11.2					
N/A	04-Oct-2024	7.5	There is a local file inclusion vulnerability in Esri Portal for ArcGIS 11.2. 11.1, 11.0	https://www.esri.com/arcgis-blog/products/t	A-ESR-PORT-211024/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 10.9.1 that may allow a remote, unauthenticated attacker to craft a URL that could potentially disclose sensitive configuration information by reading internal files. **CVE ID: CVE-2024-38040**	rust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	
Vendor: essamamdani					
Product: advanced_blocks_pro					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	5.4	The Advanced Blocks Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. **CVE ID: CVE-2024-9074**	N/A	A-ESS-ADVA-211024/646
Vendor: Flatpress					
Product: flatpress					
Affected Version(s): * Up to (excluding) 1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-2024	4.8	Cross Site Scripting vulnerability in flatpress CMS Flatpress v1.3 allows a remote attacker to execute arbitrary code via a crafted payload to the file name parameter. **CVE ID: CVE-2024-31835**	N/A	A-FLA-FLAT-211024/647
Vendor: Foxit					
Product: pdf_reader					
Affected Version(s): 2024.1.0.23997					
Use After	02-Oct-2024	8.8	A use-after-free	N/A	A-FOX-PDF -

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			vulnerability exists in the way Foxit Reade 2024.1.0.23997 handles a checkbox field object. A specially crafted Javascript code inside a malicious PDF document can trigger this vulnerability, which can lead to memory corruption and result in arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled. **CVE ID: CVE-2024-28888**		211024/648
Vendor: gdpr-extensions					
Product: consent_manager					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	5.4	The GDPR-Extensions-com – Consent Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. **CVE ID: CVE-2024-9072**	N/A	A-GDP-CONS-211024/649
Vendor: Gnome					
Product: libgsf					
Affected Version(s): 1.14.52					
Integer Overflow or	03-Oct-2024	7.8	An integer overflow vulnerability exists in the	N/A	A-GNO-LIBG-211024/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Compound Document Binary File format parser of v1.14.52 of the GNOME Project G Structured File Library (libgsf). A specially crafted file can result in an integer overflow that allows for a heap-based buffer overflow when processing the sector allocation table. This can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID: CVE-2024-42415**		
Integer Overflow or Wraparound	03-Oct-2024	7.8	An integer overflow vulnerability exists in the Compound Document Binary File format parser of the GNOME Project G Structured File Library (libgsf) version v1.14.52. A specially crafted file can result in an integer overflow when processing the directory from the file that allows for an out-of-bounds index to be used when reading and writing to an array. This can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID: CVE-2024-36474**	N/A	A-GNO-LIBG-211024/651
Vendor: Goldplugins					
Product: custom_banners					
Affected Version(s): * Up to (including) 3.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-2024	6.1	The Custom Banners plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.3. This makes it possible for unauthenticated attackers	N/A	A-GOL-CUST-211024/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-8799**		
Vendor: happyplugins					
Product: shortcodes_anywhere					
Affected Version(s): * Up to (including) 1.0.1					
Improper Control of Generation of Code ('Code Injection')	10-Oct-2024	7.3	The Shortcodes AnyWhere plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.0.1. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes. **CVE ID: CVE-2024-9581**	N/A	A-HAP-SHOR-211024/653
Vendor: hcltech					
Product: connections					
Affected Version(s): 7.0					
N/A	09-Oct-2024	5.7	HCL Connections is vulnerable to an information disclosure vulnerability which could allow a user to obtain sensitive information they are not entitled to because of improperly handling the request data. **CVE ID: CVE-2024-30118**	https://support.hcl-software.com/csm?id=kb_article&sysparm_article=KB0114302	A-HCL-CONN-211024/654
Affected Version(s): 8.0					
N/A	09-Oct-2024	5.7	HCL Connections is vulnerable to an information disclosure vulnerability which could	https://support.hcl-software.com/csm?id=kb_article	A-HCL-CONN-211024/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a user to obtain sensitive information they are not entitled to because of improperly handling the request data. **CVE ID: CVE-2024-30118**	&sysparm_article=KB0114302	
Vendor: hypestudio					
Product: social_web_suite					
Affected Version(s): * Up to (excluding) 4.1.12					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Oct-2024	7.5	The Social Web Suite – Social Media Auto Post, Social Media Auto Publish plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 4.1.11 via the download_log function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. **CVE ID: CVE-2024-8352**	https://plugins.trac.wordpress.org/changeset/3155593/social-web-suite/trunk?old=3068377&old_path=%2Fsocial-web-suite%2Ftrunk	A-HYP-SOCI-211024/656
Vendor: ibericode					
Product: mailchimp_top_bar					
Affected Version(s): * Up to (excluding) 1.6.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-2024	6.1	The MC4WP: Mailchimp Top Bar plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.6.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9210**	N/A	A-IBE-MAIL-211024/657

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: icegram					
Product: email_subscribers_\&_newsletters					
Affected Version(s): * Up to (excluding) 5.7.35					
Improper Control of Generation of Code ('Code Injection')	02-Oct-2024	6.3	The Email Subscribers by Icegram Express – Email Marketing, Newsletters, Automation for WordPress & WooCommerce plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 5.7.34. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes. **CVE ID: CVE-2024-8254**	https://plugins.trac.wordpress.org/changeset/3157336/	A-ICE-EMAI-211024/658
Vendor: icopydoc					
Product: yml_for_yandex_market					
Affected Version(s): * Up to (excluding) 4.7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-2024	6.1	The YML for Yandex Market plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'page' parameter in all versions up to, and including, 4.7.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9378**	https://plugins.trac.wordpress.org/changeset/3160483/yml-for-yandex-market/trunk/classes/system/pages/settings-page/class-y4ym-settings-page-feeds-wp-list-table.php	A-ICO-YML_-211024/659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: idiom					
Product: easy_social_share_buttons					
Affected Version(s): * Up to (including) 1.4.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	The Easy Social Share Buttons plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.4.5. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-8729**	N/A	A-IDI-EASY-211024/660
Vendor: indutny					
Product: elliptic					
Affected Version(s): * Up to (excluding) 6.5.6					
Improper Verification of Cryptographic Signature	10-Oct-2024	9.1	The verify function in lib/elliptic/eddsa/index.js in the Elliptic package before 6.5.6 for Node.js omits "sig.S().gte(sig.eddsa.curve.n) || sig.S().isNeg()" validation. **CVE ID: CVE-2024-48949**	https://github.com/indutny/elliptic/commit/7ac5360118f74eb02da73bdf9f24fd0c72ff5281, https://github.com/indutny/elliptic/compare/v6.5.5...v6.5.6	A-IND-ELLI-211024/661
Vendor: internet-formation					
Product: wp-advanced-search					
Affected Version(s): * Up to (excluding) 3.3.9.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	10-Oct-2024	9.8	The WP-Advanced-Search WordPress plugin before 3.3.9.2 does not sanitize and escape the t parameter before using it in a SQL statement, allowing unauthenticated users to perform SQL injection	N/A	A-INT-WP-A-211024/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Injection')			attacks **CVE ID: CVE-2024-9796**		
Vendor: ivanti					
Product: endpoint_manager_cloud_services_appliance					
Affected Version(s): * Up to (excluding) 5.0.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Oct-2024	7.2	An OS command injection vulnerability in the admin web console of Ivanti CSA before version 5.0.2 allows a remote authenticated attacker with admin privileges to obtain remote code execution. **CVE ID: CVE-2024-9380**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-Cloud-Services-Appliance-CVE-2024-9379-CVE-2024-9380-CVE-2024-9381	A-IVA-ENDP-211024/663
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Oct-2024	7.2	SQL injection in the admin web console of Ivanti CSA before version 5.0.2 allows a remote authenticated attacker with admin privileges to run arbitrary SQL statements. **CVE ID: CVE-2024-9379**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-Cloud-Services-Appliance-CVE-2024-9379-CVE-2024-9380-CVE-2024-9381	A-IVA-ENDP-211024/664
Vendor: iworks					
Product: pwa					
Affected Version(s): * Up to (excluding) 1.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-2024	5.4	The PWA — easy way to Progressive Web App plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.6.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. **CVE ID: CVE-2024-8967**	https://plugins.trac.wordpress.org/changeset/3161056/	A-IWO-PWA-211024/665

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Jetbrains					
Product: teamcity					
Affected Version(s): * Up to (excluding) 2024.07.03					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Oct-2024	5.4	In JetBrains TeamCity before 2024.07.3 stored XSS was possible in Backup configuration settings **CVE ID: CVE-2024-47950**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-211024/666
Affected Version(s): * Up to (excluding) 2024.07.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Oct-2024	7.5	In JetBrains TeamCity before 2024.07.3 path traversal allowed backup file write to arbitrary location **CVE ID: CVE-2024-47949**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-211024/667
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Oct-2024	7.5	In JetBrains TeamCity before 2024.07.3 path traversal leading to information disclosure was possible via server backups **CVE ID: CVE-2024-47948**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-211024/668
Insufficiently Protected Credentials	08-Oct-2024	6.5	In JetBrains TeamCity before 2024.07.3 password could be exposed via Sonar runner REST API **CVE ID: CVE-2024-47161**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-211024/669
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Oct-2024	5.4	In JetBrains TeamCity before 2024.07.3 stored XSS was possible via server global settings **CVE ID: CVE-2024-47951**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-211024/670
Vendor: jkev					
Product: record_management_system					
Affected Version(s): 1.0					
Improper Neutralizati	10-Oct-2024	6.1	A vulnerability was found in SourceCodester Record	N/A	A-JKE-RECO-211024/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file sort2_user.php. The manipulation of the argument qualification leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9810**		
Vendor: jtekt					
Product: kostac_plc					
Affected Version(s): * Up to (excluding) 1.6.15.0					
Out-of-bounds Write	03-Oct-2024	7.8	Stack-based buffer overflow vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.14.0 and earlier. Having a user open a specially crafted project file which was saved using Kostac PLC Programming Software Version 1.6.9.0 and earlier may cause a denial-of-service (DoS) condition, arbitrary code execution, and/or information disclosure because the issues exist in parsing of KPP project files. **CVE ID: CVE-2024-47135**	https://www.electronics.jtekt.co.jp/en/topics/202410026928/, https://www.electronics.jtekt.co.jp/jp/topics/2024100217388/	A-JTE-KOST-211024/672
Out-of-bounds Read	03-Oct-2024	7.8	Out-of-bounds read vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.14.0 and earlier. Having a user open a specially crafted project file which was saved using Kostac PLC Programming Software	https://www.electronics.jtekt.co.jp/en/topics/202410026928/, https://www.electronics.jtekt.co.jp/jp/topics/2024100217388/	A-JTE-KOST-211024/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Version 1.6.9.0 and earlier may cause a denial-of-service (DoS) condition, arbitrary code execution, and/or information disclosure because the issues exist in parsing of KPP project files. **CVE ID: CVE-2024-47136**		
Vendor: kainelabs					
Product: youzify					
Affected Version(s): * Up to (including) 1.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	5.4	The Youzify – BuddyPress Community, User Profile, Social Network & Membership Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's youzify_media shortcode in all versions up to, and including, 1.3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-8987**	N/A	A-KAI-YOUZ-211024/674
Missing Authorization	10-Oct-2024	4.3	The Youzify – BuddyPress Community, User Profile, Social Network & Membership Plugin for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'delete_attachment' function in all versions up to, and including, 1.3.0. This makes it possible for	N/A	A-KAI-YOUZ-211024/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attackers, with Subscriber-level access and above, to delete arbitrary attachments. **CVE ID: CVE-2024-9067**		
Vendor: kau-boys					
Product: hello_world					
Affected Version(s): * Up to (excluding) 2.2.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Oct-2024	6.5	The Hello World plugin for WordPress is vulnerable to Arbitrary File Reading in all versions up to, and including, 2.1.1 via the hello_world_lyric() function. This makes it possible for authenticated attackers, with subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information. **CVE ID: CVE-2024-9224**	N/A	A-KAU-HELL-211024/676
Vendor: kraftplugins					
Product: demo_importer_plus					
Affected Version(s): * Up to (excluding) 2.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-2024	5.4	The Demo Importer Plus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. **CVE ID: CVE-2024-9172**	https://plugins.trac.wordpress.org/changeset/3160715/	A-KRA-DEMO-211024/677
Vendor: lagunaisw					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wp_users_masquerade					
Affected Version(s): * Up to (including) 2.0.0					
Missing Authentication for Critical Function	10-Oct-2024	8.8	The WP Users Masquerade plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.0.0. This is due to incorrect authentication and capability checking in the 'ajax_masq_login' function. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to log in as any existing user on the site, such as an administrator. **CVE ID: CVE-2024-9522**	N/A	A-LAG-WP_U-211024/678
Vendor: Lemonldap-ng					
Product: lemonldap					
Affected Version(s): \ Up to (excluding) 2.19.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Oct-2024	6.1	A cross-site scripting (XSS) vulnerability in LemonLDAP::NG before 2.19.3 allows remote attackers to inject arbitrary web script or HTML into the login page via a username if userControl has been set to a non-default value that allows special HTML characters. **CVE ID: CVE-2024-48933**	N/A	A-LEM-LEMO-211024/679
Vendor: Libarchive					
Product: libarchive					
Affected Version(s): * Up to (excluding) 3.7.5					
Out-of-bounds Read	10-Oct-2024	7.8	execute_filter_audio in archive_read_support_format_rar.c in libarchive before 3.7.5 allows out-of-bounds access via a crafted archive file because src can move beyond dst.	https://github.com/libarchive/libarchive/compare/v3.7.4...v3.7.5, https://github.com/libarchive/libarchive/pull/2	A-LIB-LIBA-211024/680

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-48957	149	
Out-of-bounds Read	10-Oct-2024	7.8	execute_filter_delta in archive_read_support_format_rar.c in libarchive before 3.7.5 allows out-of-bounds access via a crafted archive file because src can move beyond dst. **CVE ID: CVE-2024-48958**	https://github.com/libarchive/libarchive/compare/v3.7.4...v3.7.5, https://github.com/libarchive/libarchive/pull/2148	A-LIB-LIBA-211024/681
Vendor: librenms					
Product: librenms					
Affected Version(s): * Up to (excluding) 24.9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-2024	5.4	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Device Dependencies" feature allows authenticated users to inject arbitrary JavaScript through the device name ("hostname" parameter). This vulnerability can lead to the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and allowing unauthorized actions. This vulnerability is fixed in 24.9.0. **CVE ID: CVE-2024-47527**	https://github.com/librenms/librenms/security/advisories/GHSA-rwwc-2v8q-gc9v	A-LIB-LIBR-211024/682
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-2024	5.4	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Alert Rules" feature allows authenticated users to inject arbitrary JavaScript through the "Title" field. This vulnerability can lead to the execution of	https://github.com/librenms/librenms/commit/7620d220e48563938d869da7689b8ac3f7721490, https://github.com/librenms/librenms/security/advisories/GHSA-j2j9-7pr6-	A-LIB-LIBR-211024/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious code in the context of other users' sessions, potentially compromising their accounts and allowing unauthorized actions. This vulnerability is fixed in 24.9.0. **CVE ID: CVE-2024-47525**	xqwv	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-2024	5.4	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Alert Transports" feature allows authenticated users to inject arbitrary JavaScript through the "Details" section (which contains multiple fields depending on which transport is selected at that moment). This vulnerability can lead to the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and allowing unauthorized actions. This vulnerability is fixed in 24.9.0. **CVE ID: CVE-2024-47523**	https://github.com/librenms/librenms/commit/ee1afba003d33667981e098c83295f599d88439c, https://github.com/librenms/librenms/security/advisories/GHSA-7f84-28qh-9486	A-LIB-LIBR-211024/684
Vendor: Limesurvey					
Product: limesurvey					
Affected Version(s): * Up to (excluding) 6.5.0\+240319					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2024	6.1	Cross Site Scripting vulnerability in LimeSurvey before 6.5.0+240319 allows a remote attacker to execute arbitrary code via a lack of input validation and output encoding in the Alert Widget's message component.	https://github.com/LimeSurvey/LimeSurvey/commit/c2fd60f94bc1db275f20cbb27a3135a9bdfb7f10	A-LIM-LIME-211024/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-28710		
Affected Version(s): * Up to (excluding) 6.5.12\+240611					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2024	6.1	Cross Site Scripting vulnerability in LimeSurvey before 6.5.12+240611 allows a remote attacker to execute arbitrary code via a crafted script to the title and comment fields. **CVE ID: CVE-2024-28709**	https://github.com/LimeSurvey/LimeSurvey/commit/c844c4fba81cc26ffe6544bf095bad6252910bc0	A-LIM-LIME-211024/686
Vendor: magicbug					
Product: cloudlog					
Affected Version(s): * Up to (including) 2.6.15					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Oct-2024	9.8	A SQL Injection vulnerability was discovered in Cloudlog 2.6.15, specifically within the get_station_info()function located in the file /application/models/Oqrs_model.php. The vulnerability is exploitable via the station_id parameter. **CVE ID: CVE-2024-45999**	N/A	A-MAG-CLOU-211024/687
Vendor: matbao					
Product: wp_helper_premium					
Affected Version(s): * Up to (including) 4.6.1					
Missing Authorization	10-Oct-2024	5.3	The WP Helper Premium plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'whp_smtp_send_mail_test' function in all versions up to, and including, 4.6.1. This makes it possible for unauthenticated attackers to send emails containing any content and originating from the vulnerable WordPress instance to any	N/A	A-MAT-WP_H-211024/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recipient. **CVE ID: CVE-2024-9065**		
Vendor: mecha-cms					
Product: mecha					
Affected Version(s): 3.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Oct-2024	9.8	Mecha CMS 3.0.0 is vulnerable to Directory Traversal. An attacker can construct cookies and URIs that bypass user identity checks. Parameters can then be passed through the POST method, resulting in the Deletion of Arbitrary Files or Website Takeover. **CVE ID: CVE-2024-46446**	N/A	A-MEC-MECH-211024/689
Vendor: memberful					
Product: memberful					
Affected Version(s): * Up to (excluding) 1.73.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	5.4	The Memberful – Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'memberful_buy_subscription_link' and 'memberful_podcasts_link' shortcodes in all versions up to, and including, 1.73.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-9242**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3161020%40memberful-wp&new=3161020%40memberful-wp&sfp_email=&sfph_mail=	A-MEM-MEMB-211024/690
Vendor: michaeluno					
Product: auto_amazon_links					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 5.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	The Auto Amazon Links – Amazon Associates Affiliate Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 5.4.2. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9349**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3161302%40amazon-auto-links&new=3161302%40amazon-auto-links&sfp_email=&sfph_mail=#file5	A-MIC-AUTO-211024/691
Vendor: miguelmello					
Product: aggregator_advanced_settings					
Affected Version(s): * Up to (including) 1.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	5.4	The Aggregator Advanced Settings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. **CVE ID: CVE-2024-9368**	N/A	A-MIG-AGGR-211024/692
Vendor: Mozilla					
Product: firefox					
Affected Version(s): * Up to (excluding) 128.3.0					
N/A	01-Oct-2024	7.5	A website configured to	https://www.m	A-MOZ-FIRE-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiate a specially crafted WebTransport session could crash the Firefox process leading to a denial of service condition. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9399**	ozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-49/, https://www.mozilla.org/security/advisories/mfsa2024-50/	211024/693
Affected Version(s): * Up to (excluding) 131.0					
N/A	01-Oct-2024	7.5	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://devtools` origin. This could allow them to access cross-origin JSON content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9394**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-48/, https://www.mozilla.org/security/advisories/mfsa2024-49/	A-MOZ-FIRE-211024/694
N/A	01-Oct-2024	7.5	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://pdf.js` origin. This could allow them to access cross-origin PDF content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-48/, https://www.mozilla.org/securi	A-MOZ-FIRE-211024/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9393**	ty/advisories/mfsa2024-49/	
Improper Restriction of Rendered UI Layers or Frames	01-Oct-2024	6.1	A missing delay in directory upload UI could have made it possible for an attacker to trick a user into granting permission via clickjacking. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9397**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-49/, https://www.mozilla.org/security/advisories/mfsa2024-50/	A-MOZ-FIRE-211024/696
N/A	01-Oct-2024	5.3	By checking the result of calls to `window.open` with specifically set protocol handlers, an attacker could determine if the application which implements that protocol handler is installed. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9398**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-49/, https://www.mozilla.org/security/advisories/mfsa2024-50/	A-MOZ-FIRE-211024/697
Affected Version(s): From (including) 129.0 Up to (excluding) 131.0					
N/A	01-Oct-2024	7.5	A website configured to initiate a specially crafted WebTransport session could crash the Firefox process leading to a denial of service condition. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/m	A-MOZ-FIRE-211024/698

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-9399	fsa2024-49/, https://www.mozilla.org/security/advisories/mfsa2024-50/	
Product: firefox_esr					
Affected Version(s): * Up to (excluding) 115.16.0					
N/A	01-Oct-2024	7.5	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://devtools` origin. This could allow them to access cross-origin JSON content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9394**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-48/, https://www.mozilla.org/security/advisories/mfsa2024-49/	A-MOZ-FIRE-211024/699
N/A	01-Oct-2024	7.5	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://pdf.js` origin. This could allow them to access cross-origin PDF content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9393**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-48/, https://www.mozilla.org/security/advisories/mfsa2024-49/	A-MOZ-FIRE-211024/700
Affected Version(s): * Up to (excluding) 128.3.0					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Rendered UI Layers or Frames	01-Oct-2024	6.1	A missing delay in directory upload UI could have made it possible for an attacker to trick a user into granting permission via clickjacking. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9397**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-49/, https://www.mozilla.org/security/advisories/mfsa2024-50/	A-MOZ-FIRE-211024/701
N/A	01-Oct-2024	5.3	By checking the result of calls to `window.open` with specifically set protocol handlers, an attacker could determine if the application which implements that protocol handler is installed. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9398**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-49/, https://www.mozilla.org/security/advisories/mfsa2024-50/	A-MOZ-FIRE-211024/702
Affected Version(s): From (including) 116.0 Up to (excluding) 128.3.0					
N/A	01-Oct-2024	7.5	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://devtools` origin. This could allow them to access cross-origin JSON content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-48/, https://www.mozilla.org/security/advisories/mfsa2024-49/	A-MOZ-FIRE-211024/703

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 131. **CVE ID: CVE-2024-9394**		
N/A	01-Oct-2024	7.5	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://pdf.js` origin. This could allow them to access cross-origin PDF content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9393**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-48/, https://www.mozilla.org/security/advisories/mfsa2024-49/	A-MOZ-FIRE-211024/704
Product: thunderbird					
Affected Version(s): * Up to (excluding) 128.3					
N/A	01-Oct-2024	7.5	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://devtools` origin. This could allow them to access cross-origin JSON content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9394**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-48/, https://www.mozilla.org/security/advisories/mfsa2024-49/	A-MOZ-THUN-211024/705
N/A	01-Oct-2024	7.5	An attacker could, via a specially crafted multipart response, execute arbitrary	https://www.mozilla.org/security/advisories/m	A-MOZ-THUN-211024/706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript under the `resource://pdf.js` origin. This could allow them to access cross-origin PDF content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9393**	fsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-48/, https://www.mozilla.org/security/advisories/mfsa2024-49/	
Improper Restriction of Rendered UI Layers or Frames	01-Oct-2024	6.1	A missing delay in directory upload UI could have made it possible for an attacker to trick a user into granting permission via clickjacking. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9397**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-49/, https://www.mozilla.org/security/advisories/mfsa2024-50/	A-MOZ-THUN-211024/707
N/A	01-Oct-2024	5.3	By checking the result of calls to `window.open` with specifically set protocol handlers, an attacker could determine if the application which implements that protocol handler is installed. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9398**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-49/, https://www.mozilla.org/security/advisories/mfsa2024-50/	A-MOZ-THUN-211024/708
Affected Version(s): * Up to (excluding) 128.3.0					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Oct-2024	7.5	A website configured to initiate a specially crafted WebTransport session could crash the Firefox process leading to a denial of service condition. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9399**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-49/, https://www.mozilla.org/security/advisories/mfsa2024-50/	A-MOZ-THUN-211024/709
Affected Version(s): 129.0					
N/A	01-Oct-2024	7.5	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://devtools` origin. This could allow them to access cross-origin JSON content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9394**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-48/, https://www.mozilla.org/security/advisories/mfsa2024-49/	A-MOZ-THUN-211024/710
N/A	01-Oct-2024	7.5	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://pdf.js` origin. This could allow them to access cross-origin PDF content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-48/, https://www.m	A-MOZ-THUN-211024/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9393**	ozilla.org/security/advisories/mfsa2024-49/	
Improper Restriction of Rendered UI Layers or Frames	01-Oct-2024	6.1	A missing delay in directory upload UI could have made it possible for an attacker to trick a user into granting permission via clickjacking. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9397**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-49/, https://www.mozilla.org/security/advisories/mfsa2024-50/	A-MOZ-THUN-211024/712
N/A	01-Oct-2024	5.3	By checking the result of calls to `window.open` with specifically set protocol handlers, an attacker could determine if the application which implements that protocol handler is installed. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131. **CVE ID: CVE-2024-9398**	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/security/advisories/mfsa2024-49/, https://www.mozilla.org/security/advisories/mfsa2024-50/	A-MOZ-THUN-211024/713
Affected Version(s): From (including) 129.0 Up to (excluding) 131.0					
N/A	01-Oct-2024	7.5	A website configured to initiate a specially crafted WebTransport session could crash the Firefox process leading to a denial of service condition. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	https://www.mozilla.org/security/advisories/mfsa2024-46/, https://www.mozilla.org/security/advisories/mfsa2024-47/, https://www.mozilla.org/securi	A-MOZ-THUN-211024/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-9399	ty/advisories/mfsa2024-49/, https://www.mozilla.org/security/advisories/mfsa2024-50/	
Vendor: namogo					
Product: elementor_inline_svg					
Affected Version(s): * Up to (including) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	5.4	The Elementor Inline SVG plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.2.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. **CVE ID: CVE-2024-9064**	N/A	A-NAM-ELEM-211024/715
Vendor: openc3					
Product: cosmos					
Affected Version(s): * Up to (excluding) 5.19.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Oct-2024	6.5	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. A path traversal vulnerability inside of LocalMode's open_local_file method allows an authenticated user with adequate permissions to download any .txt via the ScreensController#show on the web server COSMOS is running on (depending on the file permissions). This vulnerability is fixed in 5.19.0.	https://github.com/OpenC3/cosmos/commit/a34e61aea5a465f0ab3e57d833ae7ff4cafd710b, https://github.com/OpenC3/cosmos/security/advisories/GHSA-8jxr-mccc-mwg8	A-OPE-COSM-211024/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-46977		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-2024	6.1	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. The login functionality contains a reflected cross-site scripting (XSS) vulnerability. This vulnerability is fixed in 5.19.0. Note: This CVE only affects Open Source Edition, and not OpenC3 COSMOS Enterprise Edition. **CVE ID: CVE-2024-43795**	https://github.com/OpenC3/cosmos/commit/762d7e0e93bdc2f340b1e42accedc78994a576e, https://github.com/OpenC3/cosmos/security/advisories/GHSA-vfj8-5pj7-2f9g	A-OPE-COSM-211024/717
Vendor: openwebui					
Product: open_webui					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	09-Oct-2024	2.7	An information disclosure vulnerability exists in open-webui version 0.3.8. The vulnerability is related to the embedding model update feature under admin settings. When a user updates the model path, the system checks if the file exists and provides different error messages based on the existence and configuration of the file. This behavior allows an attacker to enumerate file names and traverse directories by observing the error messages, leading to potential exposure of sensitive information. **CVE ID: CVE-2024-7038**	N/A	A-OPE-OPEN-211024/718
Vendor: oretnom23					
Product: online_eyewear_shop					
Affected Version(s): 1.0					
Improper Neutralizati	15-Oct-2024	9.8	A vulnerability was found in SourceCodester Online	N/A	A-ORE-ONLI-211024/719

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Special Elements used in an SQL Command ('SQL Injection')			Eyewear Shop 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/?page=reports of the component Report Viewing Page. The manipulation of the argument date leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9973**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Oct-2024	9.8	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file classes/Master.php?f=add_to_card of the component POST Request Handler. The manipulation of the argument product_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9974**	N/A	A-ORE-ONLI-211024/720
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Oct-2024	6.5	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/?page=products/view_product. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	N/A	A-ORE-ONLI-211024/721

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-9808		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Oct-2024	6.5	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been declared as critical. Affected by this vulnerability is the function delete_product of the file /classes/Master.php?f=delete_product. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9809**	N/A	A-ORE-ONLI-211024/722
Vendor: Paloaltonetworks					
Product: cortex_xdr_agent					
Affected Version(s): 8.3.0					
Improper Check for Unusual or Exceptional Conditions	09-Oct-2024	5.5	A problem with a detection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices enables a user with Windows non-administrative privileges to disable the agent. This issue may be leveraged by malware to disable the Cortex XDR agent and then to perform malicious activity. **CVE ID: CVE-2024-9469**	https://security.paloaltonetworks.com/CVE-2024-9469	A-PAL-CORT-211024/723
Affected Version(s): 8.4.0					
Improper Check for Unusual or Exceptional Conditions	09-Oct-2024	5.5	A problem with a detection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices enables a user with Windows non-administrative privileges to disable the agent. This issue may be leveraged by malware to disable the	https://security.paloaltonetworks.com/CVE-2024-9469	A-PAL-CORT-211024/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cortex XDR agent and then to perform malicious activity. **CVE ID: CVE-2024-9469**		
Affected Version(s): From (including) 7.9 Up to (excluding) 7.9.102					
Improper Check for Unusual or Exceptional Conditions	09-Oct-2024	5.5	A problem with a detection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices enables a user with Windows non-administrative privileges to disable the agent. This issue may be leveraged by malware to disable the Cortex XDR agent and then to perform malicious activity. **CVE ID: CVE-2024-9469**	https://security.paloaltonetworks.com/CVE-2024-9469	A-PAL-CORT-211024/725
Product: expedition					
Affected Version(s): From (including) 1.2.0 Up to (excluding) 1.2.96					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Oct-2024	9.1	An SQL injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to reveal Expedition database contents, such as password hashes, usernames, device configurations, and device API keys. With this, attackers can also create and read arbitrary files on the Expedition system. **CVE ID: CVE-2024-9465**	https://security.paloaltonetworks.com/PAN-SA-2024-0010	A-PAL-EXPE-211024/726
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Oct-2024	7.5	An OS command injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to run arbitrary OS commands as root in Expedition, resulting in disclosure of usernames, cleartext passwords, device configurations, and device API keys of PAN-OS	https://security.paloaltonetworks.com/PAN-SA-2024-0010	A-PAL-EXPE-211024/727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firewalls. **CVE ID: CVE-2024-9463**		
Cleartext Storage of Sensitive Information	09-Oct-2024	6.5	A cleartext storage of sensitive information vulnerability in Palo Alto Networks Expedition allows an authenticated attacker to reveal firewall usernames, passwords, and API keys generated using those credentials. **CVE ID: CVE-2024-9466**	https://security.paloaltonetworks.com/PAN-SA-2024-0010	A-PAL-EXPE-211024/728
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Oct-2024	6.5	An OS command injection vulnerability in Palo Alto Networks Expedition allows an authenticated attacker to run arbitrary OS commands as root in Expedition, resulting in disclosure of usernames, cleartext passwords, device configurations, and device API keys of PAN-OS firewalls. **CVE ID: CVE-2024-9464**	https://security.paloaltonetworks.com/PAN-SA-2024-0010	A-PAL-EXPE-211024/729
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Oct-2024	6.1	A reflected XSS vulnerability in Palo Alto Networks Expedition enables execution of malicious JavaScript in the context of an authenticated Expedition user's browser if that user clicks on a malicious link, allowing phishing attacks that could lead to Expedition browser session theft. **CVE ID: CVE-2024-9467**	https://security.paloaltonetworks.com/PAN-SA-2024-0010	A-PAL-EXPE-211024/730
Product: globalprotect					
Affected Version(s): 6.3.0					
N/A	09-Oct-2024	7.8	A privilege escalation vulnerability in the Palo Alto Networks GlobalProtect app on Windows allows a locally authenticated non-	https://security.paloaltonetworks.com/CVE-2024-9473	A-PAL-GLOB-211024/731

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrative Windows user to escalate their privileges to NT AUTHORITY/SYSTEM through the use of the repair functionality offered by the .msi file used to install GlobalProtect. **CVE ID: CVE-2024-9473**		
Affected Version(s): 6.3.1					
N/A	09-Oct-2024	7.8	A privilege escalation vulnerability in the Palo Alto Networks GlobalProtect app on Windows allows a locally authenticated non-administrative Windows user to escalate their privileges to NT AUTHORITY/SYSTEM through the use of the repair functionality offered by the .msi file used to install GlobalProtect. **CVE ID: CVE-2024-9473**	https://security.paloaltonetworks.com/CVE-2024-9473	A-PAL-GLOB-211024/732
Affected Version(s): From (including) 5.1 Up to (excluding) 6.2.5					
N/A	09-Oct-2024	7.8	A privilege escalation vulnerability in the Palo Alto Networks GlobalProtect app on Windows allows a locally authenticated non-administrative Windows user to escalate their privileges to NT AUTHORITY/SYSTEM through the use of the repair functionality offered by the .msi file used to install GlobalProtect. **CVE ID: CVE-2024-9473**	https://security.paloaltonetworks.com/CVE-2024-9473	A-PAL-GLOB-211024/733
Vendor: petershaw					
Product: lh_copy_media_file					
Affected Version(s): * Up to (excluding) 1.09					
Improper	01-Oct-2024	6.1	The LH Copy Media File	N/A	A-PET-LH_C-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.08. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9220**		211024/734
Vendor: plainware					
Product: shiftcontroller					
Affected Version(s): * Up to (excluding) 4.9.67					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	The ShiftController Employee Shift Scheduling plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via URL keys in all versions up to, and including, 4.9.66 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9435**	https://plugins.trac.wordpress.org/changeset/3161880/	A-PLA-SHIF-211024/735
Vendor: plugingarden					
Product: wp_easy_gallery					
Affected Version(s): * Up to (including) 4.8.5					
Improper Neutralization of Special Elements	01-Oct-2024	8.8	The WP Easy Gallery – WordPress Gallery Plugin plugin for WordPress is vulnerable to time-based	N/A	A-PLU-WP_E-211024/736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			SQL Injection via the 'key' parameter in all versions up to, and including, 4.8.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-9018**		
Vendor: Progress					
Product: telerik_reporting					
Affected Version(s): * Up to (excluding) 10.2.24.806					
Weak Password Requirements	09-Oct-2024	8.8	In Progress® Telerik® Report Server versions prior to 2024 Q3 (10.2.24.806), a password brute forcing attack is possible through weak password requirements. **CVE ID: CVE-2024-7293**	https://docs.telerik.com/report-server/knowledge-base/weak-password-requirement-cve-2024-7293	A-PRO-TELE-211024/737
N/A	09-Oct-2024	6.5	In Progress® Telerik® Report Server versions prior to 2024 Q3 (10.2.24.806), an HTTP DoS attack is possible on anonymous endpoints without rate limiting. **CVE ID: CVE-2024-7294**	https://docs.telerik.com/report-server/knowledge-base/uncontrolled-resource-consumption-cve-2024-7294	A-PRO-TELE-211024/738
Affected Version(s): * Up to (excluding) 18.2.24.924					
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe	09-Oct-2024	8.8	In Progress Telerik Reporting versions prior to 2024 Q3 (18.2.24.924), a code execution attack is possible through object injection via an insecure type resolution vulnerability.	https://docs.telerik.com/reporting/knowledge-base/insecure-type-resolution-cve-2024-8014	A-PRO-TELE-211024/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reflection')			**CVE ID: CVE-2024-8014**		
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	09-Oct-2024	7.8	In Progress Telerik Reporting versions prior to 2024 Q3 (18.2.24.924), a code execution attack is possible using object injection via insecure expression evaluation. **CVE ID: CVE-2024-8048**	https://docs.telerik.com/reporting/knowledge-base/insecure-expression-evaluation-cve-2024-8048	A-PRO-TELE-211024/740
Affected Version(s): * Up to (including) 18.2.24.924					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Oct-2024	7.8	In Progress Telerik Reporting versions prior to 2024 Q3 (18.2.24.924), a command injection attack is possible through improper neutralization of hyperlink elements. **CVE ID: CVE-2024-7840**	https://docs.telerik.com/reporting/knowledge-base/command-injection-cve-2024-7840	A-PRO-TELE-211024/741
Product: telerik_report_server					
Affected Version(s): * Up to (excluding) 10.2.24.806					
Improper Restriction of Excessive Authentication Attempts	09-Oct-2024	8.8	In Progress® Telerik® Report Server versions prior to 2024 Q3 (10.2.24.806), a credential stuffing attack is possible through improper restriction of excessive login attempts. **CVE ID: CVE-2024-7292**	https://docs.telerik.com/report-server/knowledge-base/improper-restriction-of-excessive-login-attempts-cve-2024-7292	A-PRO-TELE-211024/742
Affected Version(s): * Up to (excluding) 10.2.24.924					
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	09-Oct-2024	7.2	In Progress Telerik Report Server versions prior to 2024 Q3 (10.2.24.924), a remote code execution attack is possible through object injection via an insecure type resolution vulnerability. **CVE ID: CVE-2024-8015**	https://docs.telerik.com/report-server/knowledge-base/insecure-type-resolution-cve-2024-8015	A-PRO-TELE-211024/743
Vendor: prontotools					
Product: login_logout_shortcode					
Affected Version(s): * Up to (including) 1.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	5.4	The Login Logout Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' parameter in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-9421**	N/A	A-PRO-LOGI-211024/744
Vendor: quarka					
Product: qa_analytics					
Affected Version(s): * Up to (including) 4.1.0.0					
Missing Authorization	10-Oct-2024	5.3	The QA Analytics – Web Analytics Tool with Heatmaps & Session Replay Across All Pages plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ajax_save_plugin_config() function in all versions up to, and including, 4.1.0.0. This makes it possible for unauthenticated attackers to update the plugin's settings. **CVE ID: CVE-2024-8513**	N/A	A-QUA-QA_A-211024/745
Vendor: randygaul					
Product: cute_png					
Affected Version(s): 1.05					
Out-of-bounds Write	01-Oct-2024	7.8	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_chunk() function at cute_png.h. **CVE ID: CVE-2024-46276**	N/A	A-RAN-CUTE-211024/746

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Oct-2024	7.8	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_block() function at cute_png.h. **CVE ID: CVE-2024-46267**	N/A	A-RAN-CUTE-211024/747
Out-of-bounds Write	01-Oct-2024	7.8	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_find() function at cute_png.h. **CVE ID: CVE-2024-46264**	N/A	A-RAN-CUTE-211024/748
Out-of-bounds Write	01-Oct-2024	7.8	cute_png v1.05 was discovered to contain a stack overflow via the cp_dynamic() function at cute_png.h. **CVE ID: CVE-2024-46263**	N/A	A-RAN-CUTE-211024/749
Out-of-bounds Write	01-Oct-2024	7.8	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_make32() function at cute_png.h. **CVE ID: CVE-2024-46261**	N/A	A-RAN-CUTE-211024/750
Out-of-bounds Write	01-Oct-2024	7.8	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_unfilter() function at cute_png.h. **CVE ID: CVE-2024-46259**	N/A	A-RAN-CUTE-211024/751
Out-of-bounds Write	01-Oct-2024	7.8	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_load_png_mem() function at cute_png.h. **CVE ID: CVE-2024-46258**	N/A	A-RAN-CUTE-211024/752
Out-of-bounds Write	01-Oct-2024	7.8	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_stored() function at cute_png.h. **CVE ID: CVE-2024-46274**	N/A	A-RAN-CUTE-211024/753
Vendor: redefiningtheweb					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: affiliate_pro					
Affected Version(s): * Up to (excluding) 8.5.0					
Missing Authentication for Critical Function	01-Oct-2024	9.8	The WordPress & WooCommerce Affiliate Program plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 8.4.1. This is due to the rtwwwap_login_request_callback() function not properly validating a user's identity prior to authenticating them to the site. This makes it possible for unauthenticated attackers to log in as any user, including administrators, granted they have access to the administrator's email. **CVE ID: CVE-2024-9289**	N/A	A-RED-AFFI-211024/754
Vendor: remilia					
Product: re					
Affected Version(s): wp Up to (excluding) 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	5.4	The Re:WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. **CVE ID: CVE-2024-9271**	https://plugins.trac.wordpress.org/changeset/3161983/	A-REM-RE\-211024/755
Vendor: secretlab					
Product: marketing_and_seo_booster					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.9.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	5.4	The Marketing and SEO Booster plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.9.10 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. **CVE ID: CVE-2024-9066**	N/A	A-SEC-MARK-211024/756
Vendor: seopress					
Product: seopress					
Affected Version(s): * Up to (excluding) 8.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-2024	6.1	The SEOPress – On-site SEO plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 8.1.1. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9225**	https://plugins.trac.wordpress.org/changeset/3159928/wp-seopress/trunk/inc/admin/wizard/admin-wizard.php	A-SEO-SEOP-211024/757
Vendor: shilpi					
Product: client_dashboard					
Affected Version(s): * Up to (excluding) 9.7.0					
N/A	04-Oct-2024	6.5	This vulnerability exists in Shilpi Client Dashboard due	N/A	A-SHI-CLIE-211024/758

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to improper handling of multiple parameters in the API endpoint. An authenticated remote attacker could exploit this vulnerability by including multiple "userid" parameters in the API request body leading to unauthorized access of sensitive information belonging to other users. **CVE ID: CVE-2024-47651**		
Vendor: Siemens					
Product: sinec_security_monitor					
Affected Version(s): * Up to (excluding) 4.9.0					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	08-Oct-2024	9.9	A vulnerability has been identified in Siemens SINEC Security Monitor (All versions < V4.9.0). The affected application does not properly validate user input to the ```ssmctl-client``` command. This could allow an authenticated, lowly privileged remote attacker to execute arbitrary code with root privileges on the underlying OS. **CVE ID: CVE-2024-47553**	https://cert-portal.siemens.com/productcert/html/ssa-430425.html	A-SIE-SINE-211024/759
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Oct-2024	8.8	A vulnerability has been identified in Siemens SINEC Security Monitor (All versions < V4.9.0). The affected application does not properly neutralize special elements in user input to the ```ssmctl-client``` command. This could allow an authenticated, lowly privileged local attacker to execute privileged commands in the underlying OS.	N/A	A-SIE-SINE-211024/760

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-47562		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Oct-2024	5.3	A vulnerability has been identified in Siemens SINEC Security Monitor (All versions < V4.9.0). The affected application does not properly validate a file path that is supplied to an endpoint intended to create CSR files. This could allow an unauthenticated remote attacker to create files in writable directories outside the intended location and thus compromise integrity of files in those writable directories. **CVE ID: CVE-2024-47563**	N/A	A-SIE-SINE-211024/761
N/A	08-Oct-2024	4.3	A vulnerability has been identified in Siemens SINEC Security Monitor (All versions < V4.9.0). The affected application does not properly validate that user input complies with a list of allowed values. This could allow an authenticated remote attacker to compromise the integrity of the configuration of the affected application. **CVE ID: CVE-2024-47565**	N/A	A-SIE-SINE-211024/762
Product: tecnomatix_plant_simulation					
Affected Version(s): * Up to (excluding) 2302.0016					
Out-of-bounds Read	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45466**		
N/A	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45467**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/764
Out-of-bounds Read	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45463**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/765
N/A	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005).	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/766

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. **CVE ID: CVE-2024-45474**		
N/A	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. **CVE ID: CVE-2024-45475**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/767
Out-of-bounds Write	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45469**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/768
N/A	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All	https://cert-portal.siemens.com/productcert	A-SIE-TECN-211024/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. **CVE ID: CVE-2024-45472**	/html/ssa-583523.html	
Out-of-bounds Write	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45470**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/770
N/A	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45473		
Out-of-bounds Write	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45471**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/772
N/A	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45468**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/773
Out-of-bounds Read	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45465**		
Out-of-bounds Read	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45464**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/775
NULL Pointer Dereference	08-Oct-2024	3.3	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted WRL files. An attacker could leverage this vulnerability to crash the application causing denial of service condition. **CVE ID: CVE-2024-45476**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/776
Affected Version(s): From (including) 2303.0000 Up to (excluding) 2404.0005					
N/A	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. **CVE ID: CVE-2024-45475**		
Out-of-bounds Read	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45463**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/778
Out-of-bounds Write	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45469**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/779
Out-of-bounds Write	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45470**		
N/A	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45467**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/781
Out-of-bounds Read	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45466**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/782
N/A	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix	https://cert-portal.siemens.c	A-SIE-TECN-211024/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. **CVE ID: CVE-2024-45472**	om/productcert /html/ssa-583523.html	
Out-of-bounds Write	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45471**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/784
Out-of-bounds Read	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/785

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45465		
N/A	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. **CVE ID: CVE-2024-45473**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/786
Out-of-bounds Read	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. **CVE ID: CVE-2024-45464**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/787
N/A	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. This could allow an attacker to execute code in the	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/788

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID: CVE-2024-45468**		
N/A	08-Oct-2024	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. **CVE ID: CVE-2024-45474**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/789
NULL Pointer Dereference	08-Oct-2024	3.3	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted WRL files. An attacker could leverage this vulnerability to crash the application causing denial of service condition. **CVE ID: CVE-2024-45476**	https://cert-portal.siemens.com/productcert/html/ssa-583523.html	A-SIE-TECN-211024/790
Vendor: sigmadevs					
Product: easy_demo_importer					
Affected Version(s): * Up to (excluding) 1.1.3					
Improper Neutralization of Input During Web Page Generation	04-Oct-2024	5.4	The Easy Demo Importer – A Modern One-Click Demo Import Solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all	https://plugins.trac.wordpress.org/changeset/3162305/	A-SIG-EASY-211024/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			versions up to, and including, 1.1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. **CVE ID: CVE-2024-9071**		
Vendor: soplanning					
Product: soplanning					
Affected Version(s): * Up to (excluding) 1.45					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2024	6.5	SQL injection vulnerability in SOPlanning <1.45, via /soplanning/www/user_groupes.php in the by parameter, which could allow a remote user to submit a specially crafted query, allowing an attacker to retrieve all the information stored in the DB. **CVE ID: CVE-2024-9574**	N/A	A-SOP-SOPL-211024/792
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2024	6.5	SQL injection vulnerability in SOPlanning <1.45, through /soplanning/www/groupe_list.php, in the by parameter, which could allow a remote user to send a specially crafted query and extract all the information stored on the server. **CVE ID: CVE-2024-9573**	N/A	A-SOP-SOPL-211024/793
Improper Neutralization of Input During Web Page Generation	07-Oct-2024	5.4	Cross-Site Scripting (XSS) vulnerability in SOPlanning <1.45, due to lack of proper validation of user input via /soplanning/www/process/xajax_server.php, affecting	N/A	A-SOP-SOPL-211024/794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			multiple parameters. This could allow a remote user to send a specially crafted query to an authenticated user and partially take control of their browser session. **CVE ID: CVE-2024-9571**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2024	5.4	Cross-Site Scripting (XSS) vulnerability in SOPlanning <1.45, due to lack of proper validation of user input via /soplanning/www/process/groupe_save.php, in the groupe_id parameter. This could allow a remote user to send a specially crafted query to an authenticated user and steal their session details. **CVE ID: CVE-2024-9572**	N/A	A-SOP-SOPL-211024/795
Vendor: sparkshop					
Product: sparkshop					
Affected Version(s): * Up to (including) 1.1.6					
N/A	09-Oct-2024	7.5	A loop hole in the payment logic of Sparkshop v1.16 allows attackers to arbitrarily modify the number of products. **CVE ID: CVE-2024-46307**	N/A	A-SPA-SPAR-211024/796
Vendor: sulu					
Product: sulu					
Affected Version(s): 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Sulu is a PHP content management system. Sulu is vulnerable against XSS whereas a low privileged user with access to the "Media" section can upload an SVG file with a malicious payload. Once uploaded and accessed, the malicious javascript will be executed on the victims' (other users including admins)	https://github.com/sulu/sulu/commit/ca72f75eebe41ea7726624d8aea7da6c425f1eb9, https://github.com/sulu/sulu/security/advisories/GHSA-255w-87rh-rg44	A-SUL-SULU-211024/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			browsers. This issue is fixed in 2.6.5. **CVE ID: CVE-2024-47618**		
Affected Version(s): 2.5.20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	Sulu is a PHP content management system. This vulnerability allows an attacker to inject arbitrary HTML/JavaScript code through the media download URL in Sulu CMS. It affects the SuluMediaBundle component. The vulnerability is a Reflected Cross-Site Scripting (XSS) issue, which could potentially allow attackers to steal sensitive information, manipulate the website's content, or perform actions on behalf of the victim. This vulnerability is fixed in 2.6.5 and 2.5.21. **CVE ID: CVE-2024-47617**	https://github.com/sulu/sulu/commit/eeacd14b6cf55f710084788140d40ebb00314b29, https://github.com/sulu/sulu/security/advisories/GHSA-6784-9c82-vr85	A-SUL-SULU-211024/798
Affected Version(s): 2.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	Sulu is a PHP content management system. This vulnerability allows an attacker to inject arbitrary HTML/JavaScript code through the media download URL in Sulu CMS. It affects the SuluMediaBundle component. The vulnerability is a Reflected Cross-Site Scripting (XSS) issue, which could potentially allow attackers to steal sensitive information, manipulate the website's content, or perform actions on behalf of the victim. This vulnerability is fixed in 2.6.5 and 2.5.21.	https://github.com/sulu/sulu/commit/eeacd14b6cf55f710084788140d40ebb00314b29, https://github.com/sulu/sulu/security/advisories/GHSA-6784-9c82-vr85	A-SUL-SULU-211024/799

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-47617		
Affected Version(s): From (excluding) 2.0.0 Up to (excluding) 2.6.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Sulu is a PHP content management system. Sulu is vulnerable against XSS whereas a low privileged user with access to the "Media" section can upload an SVG file with a malicious payload. Once uploaded and accessed, the malicious javascript will be executed on the victims' (other users including admins) browsers. This issue is fixed in 2.6.5. **CVE ID: CVE-2024-47618**	https://github.com/sulu/sulu/commit/ca72f75eebe41ea7726624d8aea7da6c425f1eb9, https://github.com/sulu/sulu/security/advisories/GHSA-255w-87rh-rg44	A-SUL-SULU-211024/800
Vendor: syracom					
Product: secure_login					
Affected Version(s): * Up to (including) 3.1.4.5					
N/A	10-Oct-2024	5.9	The Syracom Secure Login (2FA) plugin for Jira, Confluence, and Bitbucket through 3.1.4.5 allows remote attackers to easily brute-force the 2FA PIN via the plugins/servlet/twofactor/public/pinvalidation endpoint. The last 30 and the next 30 tokens are valid. **CVE ID: CVE-2024-48942**	https://syracom-bee.atlassian.net/wiki/spaces/SL/pages/3236560898/2024-09-16+-+Secure+Login+security+advisory+-+Insecure+default+configuration	A-SYR-SECU-211024/801
N/A	10-Oct-2024	5.4	The Syracom Secure Login (2FA) plugin for Jira, Confluence, and Bitbucket through 3.1.4.5 allows remote attackers to bypass 2FA by interacting with the /rest endpoint of Jira, Confluence, or Bitbucket. In the default configuration, /rest is allowlisted. **CVE ID: CVE-2024-48941**	https://syracom-bee.atlassian.net/wiki/spaces/SL/pages/3236560898/2024-09-16+-+Secure+Login+security+advisory+-+Insecure+default+configuration	A-SYR-SECU-211024/802
Vendor: techbanker					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: captcha_bank					
Affected Version(s): * Up to (including) 4.0.36					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	The WordPress Captcha Plugin by Captcha Bank plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 4.0.36. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9375**	N/A	A-TEC-CAPT-211024/803
Vendor: templateinvaders					
Product: ti_woocommerce_wishlist					
Affected Version(s): * Up to (including) 2.8.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Oct-2024	7.5	The TI WooCommerce Wishlist WordPress plugin through 2.8.2 is vulnerable to SQL Injection due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-9156**	N/A	A-TEM-TI_W-211024/804
Vendor: themegrill					
Product: magazine_blocks					
Affected Version(s): * Up to (excluding) 1.3.15					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-2024	6.1	The Magazine Blocks – Blog Designer, Magazine & Newspaper Website Builder, Page Builder with Posts Blocks, Post Grid plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.3.14. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9218**	https://plugins.trac.wordpress.org/changeset/3161000/#file13	A-THE-MAGA-211024/805
Vendor: themes4wp					
Product: popularis_extra					
Affected Version(s): * Up to (excluding) 1.2.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	The Popularis Extra plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.2.6. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9353**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3161466%40popularis-extra&new=3161466%40popularis-extra&sfp_email=&sfph_mail=	A-THE-POPU-211024/806
Vendor: total-soft					
Product: ts_poll					
Affected Version(s): * Up to (excluding) 2.4.1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Oct-2024	7.2	The TS Poll – Survey, Versus Poll, Image Poll, Video Poll plugin for WordPress is vulnerable to SQL Injection via the 'orderby' parameter in all versions up to, and including, 2.3.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-9022**	N/A	A-TOT-TS_P-211024/807
Vendor: tychesoftwares					
Product: product_delivery_date_for_woocommerce					
Affected Version(s): * Up to (excluding) 2.7.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	The Product Delivery Date for WooCommerce – Lite plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.7.3. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This is only exploitable when notices are present. **CVE ID: CVE-2024-9345**	https://plugins.trac.wordpress.org/changeset/3161353/product-delivery-date-for-woocommerce-lite/tags/2.7.4/includes/component/pro-notices-in-lite/ts-pro-notices.php	A-TYC-PROD-211024/808
Vendor: ultimatemember					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ultimate_member					
Affected Version(s): * Up to (excluding) 2.8.7					
Cross-Site Request Forgery (CSRF)	04-Oct-2024	4.3	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.8.6. This is due to missing or incorrect nonce validation on the admin_init or user_action_hook function. This makes it possible for unauthenticated attackers to modify a users membership status via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-8520**	https://github.com/ultimatemember/ultimatember/pull/1549, https://plugins.trac.wordpress.org/changeset/3160947/ultimate-member/trunk/includes/admin/class-admin.php	A-ULT-ULTI-211024/809
Vendor: veertu					
Product: anka_build_cloud					
Affected Version(s): 1.42.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Oct-2024	7.5	A directory traversal vulnerability exists in the archive download functionality of Veertu Anka Build 1.42.0. A specially crafted HTTP request can lead to a disclosure of arbitrary files. An attacker can make an unauthenticated HTTP request to exploit this vulnerability. **CVE ID: CVE-2024-41163**	N/A	A-VEE-ANKA-211024/810
Improper Limitation of a Pathname to a Restricted	03-Oct-2024	7.5	A directory traversal vulnerability exists in the log files download functionality of Veertu Anka Build 1.42.0. A specially	N/A	A-VEE-ANKA-211024/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			crafted HTTP request can result in a disclosure of arbitrary files. An attacker can make an unauthenticated HTTP request to trigger this vulnerability. **CVE ID: CVE-2024-41922**		
Vendor: visser					
Product: store_exporter_for_woocommerce					
Affected Version(s): * Up to (including) 2.7.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-2024	6.1	The Store Exporter for WooCommerce – Export Products, Export Orders, Export Subscriptions, and More plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.7.2.1. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-8793**	N/A	A-VIS-STOR-211024/812
Vendor: vowelweb					
Product: ibtana					
Affected Version(s): * Up to (excluding) 1.2.4.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-2024	5.4	The Ibtana – WordPress Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' attribute within the 'wp:ive/ive-productscarousel' Gutenberg block in all versions up to, and including, 1.2.4.4 due to insufficient input	https://plugins.trac.wordpress.org/browser/ibtana-visual-editor/trunk/dist/blocks.build.js, https://plugins.trac.wordpress.org/changeset/3160421/	A-VOW-IBTA-211024/813

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-8282**		
Vendor: Webkul					
Product: krayin_crm					
Affected Version(s): 1.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2024	4.8	Krayin CRM v1.3.0 is vulnerable to Cross Site Scripting (XSS) via the organization name field in /admin/contacts/organizations/edit/2. **CVE ID: CVE-2024-45932**	N/A	A-WEB-KRAY-211024/814
Vendor: wpblockshub					
Product: wp_blocks_hub					
Affected Version(s): * Up to (including) 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	5.4	The WP Blocks Hub plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. **CVE ID: CVE-2024-9372**	N/A	A-WPB-WP_B-211024/815
Vendor: wpbookingcalendar					
Product: wp_booking_calendar					
Affected Version(s): * Up to (excluding) 10.6.1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	4.8	The WP Booking Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 10.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. In addition, site administrators have the option to grant lower-level users with access to manage the plugin's settings which may extend this vulnerability to those users. **CVE ID: CVE-2024-9306**	N/A	A-WPB-WP_B-211024/816
Vendor: wpfactory					
Product: maximum_products_per_user_for_woocommerce					
Affected Version(s): * Up to (excluding) 4.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	The Maximum Products per User for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 4.2.8. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a	https://plugins.trac.wordpress.org/changeset/3164534/maximum-products-per-user-for-woocommerce/tags/4.2.9/includes/class-alg-wc-mppu-users.php	A-WPF-MAXI-211024/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			link. **CVE ID: CVE-2024-9205**		
Product: products\,_order_\&_customers_export_for_woocommerce					
Affected Version(s): * Up to (excluding) 2.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2024	6.1	The Products, Order & Customers Export for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.0.15. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9377**	https://plugins.trac.wordpress.org/changeset/3164996/	A-WPF-PROD-211024/818
Product: quantity_dynamic_pricing_\&_bulk_discounts_for_woocommerce					
Affected Version(s): * Up to (excluding) 3.8.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	6.1	The Quantity Dynamic Pricing & Bulk Discounts for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.8.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-9384**	https://plugins.trac.wordpress.org/changeset/3161269/wholesale-pricing-woocommerce/tags/3.8.1/includes/settings/class-alg-wc-wholesale-pricing-settings-per-product.php	A-WPF-QUAN-211024/819

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wpuserplus					
Product: userplus					
Affected Version(s): * Up to (including) 2.0					
N/A	10-Oct-2024	9.8	The UserPlus plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 2.0 due to insufficient restriction on the 'form_actions' and 'userplus_update_user_profile' functions. This makes it possible for unauthenticated attackers to specify their user role by supplying the 'role' parameter during a registration. **CVE ID: CVE-2024-9518**	N/A	A-WPU-USER-211024/820
N/A	10-Oct-2024	7.2	The UserPlus plugin for WordPress is vulnerable to unauthorized modification of data due to an improper capability check on the 'save_metabox_form' function in versions up to, and including, 2.0. This makes it possible for authenticated attackers, with editor-level permissions or above, to update the registration form role to administrator, which leads to privilege escalation. **CVE ID: CVE-2024-9519**	N/A	A-WPU-USER-211024/821
Missing Authorization	10-Oct-2024	5.4	The UserPlus plugin for WordPress is vulnerable to unauthorized access, modification, and loss of data due to a missing capability check on multiple functions in all versions up to, and including, 2.0. This makes it possible for authenticated attackers with subscriber-level permissions or above, to	N/A	A-WPU-USER-211024/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			add, modify, or delete user meta and plugin options. **CVE ID: CVE-2024-9520**		
Vendor: yoginetwork					
Product: rabbitloader					
Affected Version(s): * Up to (excluding) 2.21.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-2024	6.1	The RabbitLoader – Website Speed Optimization for improving Core Web Vital metrics with Cache, Image Optimization, and more plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.21.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-8800**	https://plugins.trac.wordpress.org/changeset/3160267/	A-YOG-RABB-211024/823
Vendor: Zimbra					
Product: collaboration					
Affected Version(s): * Up to (excluding) 8.8.15					
Incorrect Authorization	02-Oct-2024	9.8	The postjournal service in Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1 sometimes allows unauthenticated users to execute commands. **CVE ID: CVE-2024-45519**	N/A	A-ZIM-COLL-211024/824
Affected Version(s): 10.1.0					
Incorrect Authorization	02-Oct-2024	9.8	The postjournal service in Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9	N/A	A-ZIM-COLL-211024/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1 sometimes allows unauthenticated users to execute commands. **CVE ID: CVE-2024-45519**		
Affected Version(s): 8.8.15					
Incorrect Authorization	02-Oct-2024	9.8	The postjournal service in Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1 sometimes allows unauthenticated users to execute commands. **CVE ID: CVE-2024-45519**	N/A	A-ZIM-COLL-211024/826
Affected Version(s): 9.0.0					
Incorrect Authorization	02-Oct-2024	9.8	The postjournal service in Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1 sometimes allows unauthenticated users to execute commands. **CVE ID: CVE-2024-45519**	N/A	A-ZIM-COLL-211024/827
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.9					
Incorrect Authorization	02-Oct-2024	9.8	The postjournal service in Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1 sometimes allows unauthenticated users to execute commands. **CVE ID: CVE-2024-45519**	N/A	A-ZIM-COLL-211024/828
Hardware					
Vendor: Cisco					
Product: meraki_mx100					
Affected Version(s): -					
Uncontrolled Resource Consumptio	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco	https://sec.cloudapps.cisco.com/security/center	H-CIS-MERA-211024/829

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n			Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/830

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/832

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device. **CVE ID: CVE-2024-20509**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/834
Authorizatio	02-Oct-2024	5.3	A vulnerability in the Cisco	https://sec.clou	H-CIS-MERA-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n Bypass Through User-Controlled Key			AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	211024/835
Product: meraki_mx105					
Affected Version(s): -					
Out-of-bounds	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN	https://sec.cloudapps.cisco.com	H-CIS-MERA-211024/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-	H-CIS-MERA-211024/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/838

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/839

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/840

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device. **CVE ID: CVE-2024-20509**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/842
Product: meraki_mx250					
Affected Version(s): -					
Out-of-	02-Oct-2024	7.5	Multiple vulnerabilities in	https://sec.clou	H-CIS-MERA-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	211024/843
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-MERA-211024/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	meraki-mx-vpn-dos-QTRHzG2	
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/846

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/847

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20509		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/849
Product: meraki_mx400					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/850
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/854

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/855

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/856
Product: meraki_mx450					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/857
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/861

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/863
Product: meraki_mx600					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/864
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/866

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/868

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/869

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/870
Product: meraki_mx64					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/871
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/872

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/875

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/876

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/877
Product: meraki_mx64w					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/878
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/883

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/884
Product: meraki_mx65					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/885
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/886

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/887

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/889

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/890

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/891
Product: meraki_mx65w					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/892
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/896

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/898
Product: meraki_mx67					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/899
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/901

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/903

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/904

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/905
Product: meraki_mx67c					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/906
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/911

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/912
Product: meraki_mx67w					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/913
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/915

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/916

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/917

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/918

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/919
Product: meraki_mx68					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/920
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/924

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/925

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/926
Product: meraki_mx68cw					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/927
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/929

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/930

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/933
Product: meraki_mx68w					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/934
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/938

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/939

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/940
Product: meraki_mx75					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/941
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/945

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/947
Product: meraki_mx84					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/948
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/950

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/952

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/953

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/954
Product: meraki_mx85					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/955
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/959

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/960

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/961
Product: meraki_mx95					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/962
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/968
Product: meraki_vmx					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/969
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/973

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/974

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/975
Product: meraki_z3					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/976
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-MERA-211024/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/980

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/982
Product: meraki_z3c					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/983
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/985

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/987

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/989
Product: meraki_z4					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/990
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/991

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/993

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/996
Product: meraki_z4c					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/997
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/998

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/999

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	H-CIS-MERA-211024/1002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	H-CIS-MERA-211024/1003
Product: rv042					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1004
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1005

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1006
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	H-CIS-RV04-211024/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1008

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20523		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1010
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1012

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Product: rv042g					
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1013
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vul	H-CIS-RV04-211024/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	ns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1015

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1016
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1017

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1018

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1019
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	H-CIS-RV04-211024/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV04-211024/1021

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Product: rv320					
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20520		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1023
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1024

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1025
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	H-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/1026
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1027

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1029
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Product: rv325					
Affected Version(s): -					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1031

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1032
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vul	H-CIS-RV32-211024/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	ns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1034

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1035
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vul	H-CIS-RV32-211024/1036

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	ns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1037

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	H-CIS-RV32-211024/1038
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	H-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/1039
Product: rv340w_dual_wan_gigabit_wireless-ac_vpn_router					
Affected Version(s): -					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	H-CIS-RV34-211024/1040

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	H-CIS-RV34-211024/1041
Product: rv340_dual_wan_gigabit_vpn_router					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	H-CIS-RV34-211024/1042
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	H-CIS-RV34-211024/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Product: rv345p_dual_wan_gigabit_poe_vpn_router					
Affected Version(s): -					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	H-CIS-RV34-211024/1044
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-	H-CIS-RV34-211024/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	qE33TCms	
Product: rv345_dual_wan_gigabit_vpn_router					
Affected Version(s): -					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	H-CIS-RV34-211024/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	H-CIS-RV34-211024/1047
Vendor: Dlink					
Product: dir-605l					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. This affects the function formSetQoS of the file /goform/formSetQoS. The manipulation of the	N/A	H-DLI-DIR--211024/1048

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been declared as critical. This vulnerability affects the function formSetDomainFilter of the file /goform/formSetDomainFilter. The manipulation of the argument curTime leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9514**	N/A	H-DLI-DIR--211024/1049
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This issue affects the function formDeviceReboot of the file /goform/formDeviceReboot. The manipulation of the argument next_page leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9533**	N/A	H-DLI-DIR--211024/1050
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Oct-2024	8.8	A vulnerability has been found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This vulnerability affects the function formAdvanceSetup of the file /goform/formAdvanceSetup. The manipulation of the	N/A	H-DLI-DIR--211024/1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument webpage leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9532**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. Affected is the function formEasySetPassword of the file /goform/formEasySetPassword. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9534**	N/A	H-DLI-DIR--211024/1052
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been declared as critical. Affected by this vulnerability is the function formEasySetupWWConfig of the file /goform/formEasySetupWWConfig. The manipulation of the argument curTime leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9535**	N/A	H-DLI-DIR--211024/1053
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This issue affects the function formEasySetupWizard/formEasySetupWizard2 of the file /goform/formEasySetupWi	N/A	H-DLI-DIR--211024/1054

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			zard. The manipulation of the argument curTime leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9549**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. Affected is the function formLogDnsquery of the file /goform/formLogDnsquery. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9550**	N/A	H-DLI-DIR--211024/1055
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been declared as critical. Affected by this vulnerability is the function formSetWanL2TP of the file /goform/formSetWanL2TP. The manipulation of the argument webpage leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9551**	N/A	H-DLI-DIR--211024/1056
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been rated as critical. Affected by this issue is the function formSetWanNonLogin of the file /goform/formSetWanNonLogin. The manipulation of the argument webpage	N/A	H-DLI-DIR--211024/1057

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9552**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability classified as critical has been found in D-Link DIR-605L 2.13B01 BETA. This affects the function formdumpeasysetup of the file /goform/formdumpeasysetup. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9553**	N/A	H-DLI-DIR--211024/1058
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability, which was classified as critical, has been found in D-Link DIR-605L 2.13B01 BETA. Affected by this issue is the function formSetEasy_Wizard of the file /goform/formSetEasy_Wizard. The manipulation of the argument curTime leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9555**	N/A	H-DLI-DIR--211024/1059
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability, which was classified as critical, was found in D-Link DIR-605L 2.13B01 BETA. This affects the function formSetEnableWizard of the file /goform/formSetEnableWizard. The manipulation of	N/A	H-DLI-DIR--211024/1060

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9556**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability has been found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This vulnerability affects the function formSetWanPPPoE of the file /goform/formSetWanPPPoE. The manipulation of the argument webpage leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9557**	N/A	H-DLI-DIR--211024/1061
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This issue affects the function formSetWanPPTP of the file /goform/formSetWanPPTP. The manipulation of the argument webpage leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9558**	N/A	H-DLI-DIR--211024/1062
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. Affected is the function formWlanSetup of the file /goform/formWlanSetup. The manipulation of the argument webpage leads to buffer overflow. It is	N/A	H-DLI-DIR--211024/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9559**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability classified as critical has been found in D-Link DIR-605L 2.13B01 BETA. This affects the function formSetWAN_Wizard51/formSetWAN_Wizard52. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9561**	N/A	H-DLI-DIR--211024/1064
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability classified as critical was found in D-Link DIR-605L 2.13B01 BETA. This vulnerability affects the function formSetWizard1/formSetWizard2. The manipulation of the argument curTime leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9562**	N/A	H-DLI-DIR--211024/1065
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability, which was classified as critical, has been found in D-Link DIR-605L 2.13B01 BETA. This issue affects the function formWlanSetup_Wizard of the file /goform/formWlanSetup_Wizard. The manipulation of the argument webpage leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public	N/A	H-DLI-DIR--211024/1066

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and may be used. **CVE ID: CVE-2024-9563**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability, which was classified as critical, was found in D-Link DIR-605L 2.13B01 BETA. Affected is the function formWlanWizardSetup of the file /goform/formWlanWizardSetup. The manipulation of the argument webpage leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9564**	N/A	H-DLI-DIR--211024/1067
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability has been found in D-Link DIR-605L 2.13B01 BETA and classified as critical. Affected by this vulnerability is the function formSetPassword of the file /goform/formSetPassword. The manipulation of the argument curTime leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9565**	N/A	H-DLI-DIR--211024/1068
Product: dir-619l					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability was found in D-Link DIR-619L B1 2.06 and classified as critical. Affected by this issue is the function formEasySetTimezone of the file /goform/formEasySetTimezone. The manipulation of the argument curTime leads to buffer overflow. The	N/A	H-DLI-DIR--211024/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9570**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability, which was classified as critical, has been found in D-Link DIR-619L B1 2.06. This issue affects the function formAdvFirewall of the file /goform/formAdvFirewall. The manipulation of the argument curTime leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9567**	N/A	H-DLI-DIR--211024/1070
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability, which was classified as critical, was found in D-Link DIR-619L B1 2.06. Affected is the function formAdvNetwork of the file /goform/formAdvNetwork. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9568**	N/A	H-DLI-DIR--211024/1071
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability has been found in D-Link DIR-619L B1 2.06 and classified as critical. Affected by this vulnerability is the function formEasySetPassword of the file /goform/formEasySetPassword. The manipulation of the argument curTime leads to buffer overflow. The attack can be launched remotely. The exploit has	N/A	H-DLI-DIR--211024/1072

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. **CVE ID: CVE-2024-9569**		
Vendor: Draytek					
Product: vigor1000b					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1073
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1074
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1075
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1076
Product: vigor165					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1077
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1078
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1079
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1080
Product: vigor166					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(),	N/A	H-DRA-VIGO-211024/1081

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1082
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1083
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1084
Product: vigor2133					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow.	N/A	H-DRA-VIGO-211024/1085

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41593		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1086
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1087
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1088
Product: vigor2135					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1089
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of	N/A	H-DRA-VIGO-211024/1090

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1091
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1092
Product: vigor2620					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1093
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1094
Improper	03-Oct-2024	6.1	DrayTek Vigor3910 devices	N/A	H-DRA-VIGO-

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**		211024/1095
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1096
Product: vigor2762					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1097
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1098
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1099

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1100
Product: vigor2763					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1101
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1102
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1103
Improper Neutralization of Input During Web Page Generation ('Cross-site	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6.	N/A	H-DRA-VIGO-211024/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID: CVE-2024-41587**		
Product: vigor2765					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1105
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1106
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1107
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1108
Product: vigor2766					
Affected Version(s): -					
Out-of-bounds	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a	N/A	H-DRA-VIGO-211024/1109

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1110
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1111
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1112
Product: vigor2832					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a	N/A	H-DRA-VIGO-211024/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1114
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1115
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1116
Product: vigor2860					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1117
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to	N/A	H-DRA-VIGO-211024/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1119
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1120
Product: vigor2862					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1121
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL.	N/A	H-DRA-VIGO-211024/1122

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41594		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1123
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1124
Product: vigor2865					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1125
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1126
Improper Neutralization of Input During Web Page	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS.	N/A	H-DRA-VIGO-211024/1127

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			**CVE ID: CVE-2024-41591**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1128
Product: vigor2866					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1129
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1130
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1131
Improper Neutralization of Input During Web	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting	N/A	H-DRA-VIGO-211024/1132

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**		
Product: vigor2915					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1133
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1134
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1135
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1136
Product: vigor2925					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1137
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1138
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1139
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1140
Product: vigor2926					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(),	N/A	H-DRA-VIGO-211024/1141

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1142
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1143
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1144
Product: vigor2952					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow.	N/A	H-DRA-VIGO-211024/1145

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41593		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1146
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1147
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1148
Product: vigor2962					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1149
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of	N/A	H-DRA-VIGO-211024/1150

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1151
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1152
Product: vigor3220					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1153
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1154
Improper	03-Oct-2024	6.1	DrayTek Vigor3910 devices	N/A	H-DRA-VIGO-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**		211024/1155
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1156
Product: vigor3910					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1157
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1158
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1159

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1160
Product: vigor3912					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1161
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1162
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1163
Improper Neutralization of Input During Web Page Generation ('Cross-site	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6.	N/A	H-DRA-VIGO-211024/1164

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID: CVE-2024-41587**		
Product: vigorlte200					
Affected Version(s): -					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	H-DRA-VIGO-211024/1165
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	H-DRA-VIGO-211024/1166
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	H-DRA-VIGO-211024/1167
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	H-DRA-VIGO-211024/1168
Vendor: mediatek					
Product: mt3605					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	07-Oct-2024	4.9	In wlan driver, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998892; Issue ID: MSV-1601. **CVE ID: CVE-2024-20102**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT36-211024/1169
Product: mt6580					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT65-211024/1170
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT65-211024/1171
Product: mt6739					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**		
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1173
Product: mt6761					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1174
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1175
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1176

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**		
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1177
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1178
Product: mt6765					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1179
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1180

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**		
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1181
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1182
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1183
Product: mt6768					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**		
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1185
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1186
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1187
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699.	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20093		
Product: mt6779					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1189
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1190
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1191
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635.	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20096		
Product: mt6781					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1193
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1194
Product: mt6785					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1195
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**		
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1197
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1198
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1199
Product: mt6789					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**		
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1201
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT67-211024/1202
Product: mt6833					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1203
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**		
Product: mt6853					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1205
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1206
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1207
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**		
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1209
Product: mt6855					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1210
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1211
Product: mt6873					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/Octobe	H-MED-MT68-211024/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	r-2024	
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1213
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1214
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1215
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**		
Product: mt6877					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1217
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1218
Product: mt6879					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1219
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/Octobe	H-MED-MT68-211024/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	r-2024	
Product: mt6883					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1221
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1222
Product: mt6885					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1223
Out-of-	07-Oct-2024	4.4	In m4u, there is a possible	https://corp.me	H-MED-MT68-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Read			out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	diatek.com/product-security-bulletin/October-2024	211024/1224
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1225
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1226
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1227
Product: mt6889					
Affected Version(s): -					
Out-of-	07-Oct-2024	4.4	In m4u, there is a possible	https://corp.me	H-MED-MT68-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Read			out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	diatek.com/product-security-bulletin/October-2024	211024/1228
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1229
Product: mt6893					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1230
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1231

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6895					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1232
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT68-211024/1233
Product: mt6983					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT69-211024/1234
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894;	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT69-211024/1235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**		
Product: mt6985					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.9	In wlan driver, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998892; Issue ID: MSV-1601. **CVE ID: CVE-2024-20102**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT69-211024/1236
Product: mt6989					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.9	In wlan driver, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998892; Issue ID: MSV-1601. **CVE ID: CVE-2024-20102**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT69-211024/1237
Product: mt6990					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.9	In wlan driver, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998892; Issue ID: MSV-1601.	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT69-211024/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20102		
Product: mt7927					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.9	In wlan driver, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998892; Issue ID: MSV-1601. **CVE ID: CVE-2024-20102**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT79-211024/1239
Product: mt8385					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT83-211024/1240
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT83-211024/1241
Product: mt8666					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a	https://corp.mediatek.com/pro	H-MED-MT86-211024/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**	duct-security-bulletin/October-2024	
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1243
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1244
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1245
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1246

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**		
Product: mt8667					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1247
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1248
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1249
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**		
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1251
Product: mt8673					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1252
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1253
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**		
Product: mt8675					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1255
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1256
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1257
Product: mt8678					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.9	In wlan driver, there is a possible out of bounds read	https://corp.mediatek.com/pro	H-MED-MT86-211024/1258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper input validation. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998892; Issue ID: MSV-1601. **CVE ID: CVE-2024-20102**	duct-security-bulletin/October-2024	
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1259
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1260
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT86-211024/1261
Product: mt8766					
Affected Version(s): -					
Out-of-	07-Oct-2024	4.4	In vdec, there is a possible	https://corp.me	H-MED-MT87-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Read			out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**	diatek.com/product-security-bulletin/October-2024	211024/1262
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT87-211024/1263
Product: mt8768					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT87-211024/1264
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT87-211024/1265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8781					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT87-211024/1266
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT87-211024/1267
Product: mt8788					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT87-211024/1268
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313;	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT87-211024/1269

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**		
Product: mt8789					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT87-211024/1270
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT87-211024/1271
Product: mt8796					
Affected Version(s): -					
Out-of-bounds Read	07-Oct-2024	4.9	In wlan driver, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998892; Issue ID: MSV-1601. **CVE ID: CVE-2024-20102**	https://corp.mediatek.com/product-security-bulletin/October-2024	H-MED-MT87-211024/1272
Product: mt8893					
Affected Version(s): -					
Out-of-	07-Oct-2024	4.9	In wlan driver, there is a	https://corp.me	H-MED-MT88-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Read			possible out of bounds read due to improper input validation. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998892; Issue ID: MSV-1601. **CVE ID: CVE-2024-20102**	diatek.com/product-security-bulletin/October-2024	211024/1273
Vendor: Microchip					
Product: timeprovider_4100_grandmaster					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Oct-2024	8.8	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Microchip TimeProvider 4100 (Configuration modules) allows Command Injection.This issue affects TimeProvider 4100: from 1.0 before 2.4.7. **CVE ID: CVE-2024-9054**	https://www.microchip.com/en-us/solutions/technologies/embedded-security/how-to-report-potential-product-security-vulnerabilities/timeprovider-4100-grandmaster-rce-through-configuration-file	H-MIC-TIME-211024/1274
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Oct-2024	6.5	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Microchip TimeProvider 4100 (Data plot modules) allows SQL Injection.This issue affects TimeProvider 4100: from 1.0 before 2.4.7. **CVE ID: CVE-2024-7801**	https://www.microchip.com/en-us/solutions/technologies/embedded-security/how-to-report-potential-product-security-vulnerabilities/timeprovider-4100-grandmaster-unathenticated-sql-injection	H-MIC-TIME-211024/1275
Vendor: Qualcomm					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fastconnect_6700					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-FAST-211024/1276
Product: fastconnect_6800					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-FAST-211024/1277
Product: fastconnect_6900					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-FAST-211024/1278
Product: fastconnect_7800					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-FAST-211024/1279
Product: qam8295p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QAM8-211024/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6174a					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCA6-211024/1281
Product: qca6391					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCA6-211024/1282
Product: qca6426					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCA6-211024/1283
Product: qca6436					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCA6-211024/1284
Product: qca6574au					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCA6-211024/1285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6584au					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCA6-211024/1286
Product: qca6595					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCA6-211024/1287
Product: qca6595au					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCA6-211024/1288
Product: qca6688aq					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCA6-211024/1289
Product: qca6696					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCA6-211024/1290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6698aq					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCA6-211024/1291
Product: qcs410					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCS4-211024/1292
Product: qcs610					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCS6-211024/1293
Product: qcs6490					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-QCS6-211024/1294
Product: sa4150p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SA41-211024/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa4155p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SA41-211024/1296
Product: sa6145p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SA61-211024/1297
Product: sa6150p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SA61-211024/1298
Product: sa6155p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SA61-211024/1299
Product: sa8145p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SA81-211024/1300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa8150p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SA81-211024/1301
Product: sa8155p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SA81-211024/1302
Product: sa8195p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SA81-211024/1303
Product: sa8295p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SA82-211024/1304
Product: sd660					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SD66-211024/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sd865_5g					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SD86-211024/1306
Product: sg4150p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SG41-211024/1307
Product: snapdragon_660_mobile					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1308
Product: snapdragon_680_4g_mobile					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1309
Product: snapdragon_685_4g_mobile					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_865\+_5g_mobile					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1311
Product: snapdragon_865_5g_mobile					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1312
Product: snapdragon_870_5g_mobile					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1313
Product: snapdragon_888\+_5g_mobile					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1314
Product: snapdragon_888_5g_mobile					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_8_gen_1_mobile					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1316
Product: snapdragon_auto_5g_modem-rf					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1317
Product: snapdragon_auto_5g_modem-rf_gen_2					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1318
Product: snapdragon_x55_5g_modem-rf					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1319
Product: snapdragon_xr2_5g					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SNAP-211024/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sw5100					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SW51-211024/1321
Product: sw5100p					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SW51-211024/1322
Product: sxr2130					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-SXR2-211024/1323
Product: video_collaboration_vc1					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-VIDE-211024/1324
Product: video_collaboration_vc3					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-VIDE-211024/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcd9335					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WCD9-211024/1326
Product: wcd9341					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WCD9-211024/1327
Product: wcd9370					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WCD9-211024/1328
Product: wcd9375					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WCD9-211024/1329
Product: wcd9380					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WCD9-211024/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcd9385					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WCD9-211024/1331
Product: wcn3950					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WCN3-211024/1332
Product: wcn3980					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WCN3-211024/1333
Product: wcn3988					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WCN3-211024/1334
Product: wcn3990					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WCN3-211024/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wsa8810					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WSA8-211024/1336
Product: wsa8815					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WSA8-211024/1337
Product: wsa8830					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WSA8-211024/1338
Product: wsa8835					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	H-QUA-WSA8-211024/1339
Operating System					
Vendor: Apple					
Product: ipados					
Affected Version(s): * Up to (excluding) 18.0.1					
N/A	04-Oct-2024	5.5	A logic issue was addressed with improved validation. This issue is fixed in iOS 18.0.1 and iPadOS 18.0.1. A	https://support.apple.com/en-us/121373	O-APP-IPAD-211024/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user's saved passwords may be read aloud by VoiceOver. **CVE ID: CVE-2024-44204**		
N/A	04-Oct-2024	4.3	This issue was addressed with improved checks. This issue is fixed in iOS 18.0.1 and iPadOS 18.0.1. Audio messages in Messages may be able to capture a few seconds of audio before the microphone indicator is activated. **CVE ID: CVE-2024-44207**	https://support.apple.com/en-us/121373	O-APP-IPAD-211024/1341
Product: iphone_os					
Affected Version(s): * Up to (excluding) 18.0.1					
N/A	04-Oct-2024	5.5	A logic issue was addressed with improved validation. This issue is fixed in iOS 18.0.1 and iPadOS 18.0.1. A user's saved passwords may be read aloud by VoiceOver. **CVE ID: CVE-2024-44204**	https://support.apple.com/en-us/121373	O-APP-IPHO-211024/1342
N/A	04-Oct-2024	4.3	This issue was addressed with improved checks. This issue is fixed in iOS 18.0.1 and iPadOS 18.0.1. Audio messages in Messages may be able to capture a few seconds of audio before the microphone indicator is activated. **CVE ID: CVE-2024-44207**	https://support.apple.com/en-us/121373	O-APP-IPHO-211024/1343
Product: macos					
Affected Version(s): -					
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-APP-MACO-211024/1344

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-47418		
Out-of-bounds Write	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47417**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-APP-MACO-211024/1345
Integer Overflow or Wraparound	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47416**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-APP-MACO-211024/1346
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47415**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-APP-MACO-211024/1347
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-APP-MACO-211024/1348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47414**		
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47413**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-APP-MACO-211024/1349
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47412**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-APP-MACO-211024/1350
Out-of-bounds Write	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47410**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-APP-MACO-211024/1351
Access of Uninitialized Pointer	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-APP-MACO-211024/1352

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47411**		
Out-of-bounds Read	09-Oct-2024	5.5	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47420**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-APP-MACO-211024/1353
Out-of-bounds Read	09-Oct-2024	5.5	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47419**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-APP-MACO-211024/1354
Vendor: Cisco					
Product: meraki_mx100_firmware					
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1356

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1357

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1359

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device. **CVE ID: CVE-2024-20509**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1360
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-MERA-211024/1361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	meraki-mx-vpn-dos-QTRHzG2	
Product: meraki_mx105_firmware					
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-	O-CIS-MERA-211024/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1363

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1366

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device. **CVE ID: CVE-2024-20509**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1367
Authorization Bypass Through User-Controlled	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-MERA-211024/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Key			allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Product: meraki_mx250_firmware					
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-MERA-211024/1369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1370

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1372

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1373

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device. **CVE ID: CVE-2024-20509**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1374
Authorization Bypass Through User-	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Product: meraki_mx400_firmware					
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-MERA-211024/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1377

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1378

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device. **CVE ID: CVE-2024-20509**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1381
Authorization Bypass Through	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco	https://sec.cloudapps.cisco.com/security/center	O-CIS-MERA-211024/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
User-Controlled Key			Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Product: meraki_mx450_firmware					
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1386

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device. **CVE ID: CVE-2024-20509**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1388
Authorization Bypass	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of	https://sec.cloudapps.cisco.com	O-CIS-MERA-211024/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Through User-Controlled Key			Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Product: meraki_mx600_firmware					
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Uncontrolled Resource Consumptio	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco	https://sec.cloudapps.cisco.com/security/center	O-CIS-MERA-211024/1390

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n			Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**	/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1391

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1394

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device. **CVE ID: CVE-2024-20509**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1395
Authorizatio	02-Oct-2024	5.3	A vulnerability in the Cisco	https://sec.clou	O-CIS-MERA-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n Bypass Through User-Controlled Key			AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	211024/1396
Product: meraki_mx64w_firmware					
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Out-of-bounds	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN	https://sec.cloudapps.cisco.com	O-CIS-MERA-211024/1397

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-	O-CIS-MERA-211024/1398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**	dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1401

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device. **CVE ID: CVE-2024-20509**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1403
Product: meraki_mx64_firmware					
Affected Version(s): From (including) 17.6.0 Up to (excluding) 18.211.2					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in	https://sec.clou	O-CIS-MERA-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	211024/1404
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-MERA-211024/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	meraki-mx-vpn-dos-QTRHzG2	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**		
Affected Version(s): From (including) 17.6.0 Up to (including) 18.211.2					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1408

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1409

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intervention. **CVE ID: CVE-2024-20501**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1410
Product: meraki_mx65w_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1411
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1414

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1415

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1416

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1417
Product: meraki_mx65_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 17.6.0 Up to (excluding) 18.211.2					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1418
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1421

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1423

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1424
Product: meraki_mx67c_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1425
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1430

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1431
Product: meraki_mx67w_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1432
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1435

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1436

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1437

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1438
Product: meraki_mx67_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1439
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1441

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1442

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1444

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1445
Product: meraki_mx68cw_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1446
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1450

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1452
Product: meraki_mx68w_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1453
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1455

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1456

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1457

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1458

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1459
Product: meraki_mx68_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1460
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1463

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1465

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1466
Product: meraki_mx75_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1467
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	ecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1470

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1471

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1472

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1473
Product: meraki_mx84_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1474
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1478

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1480
Product: meraki_mx85_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1481
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1483

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1485

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1487
Product: meraki_mx95_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1488
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1490

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1492

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1493

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1494
Product: meraki_vmx_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1495
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1498

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1499

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1500

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1501
Product: meraki_z3c_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1502
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1505

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1506

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1507

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1508
Product: meraki_z3_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1509
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1513

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1514

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1515
Product: meraki_z4c_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1516
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1519

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**		
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1521

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1522
Product: meraki_z4_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.2 Up to (excluding) 18.211.2					
Double Free	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20498**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1523
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-MERA-211024/1524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20499**	ecurityAdvisory /cisco-sa-meraki-mx-vpn-dos-QTRHzG2	
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20500**		
Out-of-bounds Write	02-Oct-2024	7.5	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20501**		
Uncontrolled Resource Consumption	02-Oct-2024	7.5	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1527

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. **CVE ID: CVE-2024-20502**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-2024	5.9	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X	O-CIS-MERA-211024/1528

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the affected device. **CVE ID: CVE-2024-20509**		
Authorization Bypass Through User-Controlled Key	02-Oct-2024	5.3	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate. **CVE ID: CVE-2024-20513**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2	O-CIS-MERA-211024/1529
Product: rv042g_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0.1.17					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1530
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1532
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV04-211024/1533

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1534

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1535

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20517		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1536
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1538

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 1.0.2.03					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1539
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1540

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1542
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1543

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1545
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV04-211024/1546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1547

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.1.0.09					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1548
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV04-211024/1549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1550

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1551
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1552

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1553

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1554

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20517		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1555
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 1.1.1.06					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1557

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1558
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1560

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1561
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1564
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV04-211024/1565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 1.1.1.19					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1566

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1567
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1568

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1569

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1570
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1572

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1573

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20516		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1574
Affected Version(s): 1.2.1.13					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1575

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1576

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1577
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1578

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1580
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1583
Affected Version(s): 1.2.1.14					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1585

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1586
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1588

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1589
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1591

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1592

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20524		
Affected Version(s): 1.3.1.10					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1593
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1595

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1596
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1597

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1599
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.3.1.12					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1602
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1604

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1605
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1606

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1608
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1610

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 1.3.12.19-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1611
Out-of-	02-Oct-2024	9.1	A vulnerability in the web-	https://sec.clou	O-CIS-RV04-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/1612
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to	https://sec.clouddapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1613

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1614
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV04-211024/1615

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1616

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1617

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20524		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1618
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.3.12.6-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1620

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1621
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1623

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1624
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1627
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV04-211024/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 1.3.13.02-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1630
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1631

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1632

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1633
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1635

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20516		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1637
Affected Version(s): 1.3.2.02					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1638

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1639

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1640
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1641

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1643
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1646
Affected Version(s): 1.4.2.15					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1647

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1648

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1649
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1651

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1652
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1654

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20517		
Affected Version(s): 1.4.2.17					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1656
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1658

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1659
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1660

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1662
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 1.4.2.19					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1665
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1668
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1669

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1671
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1672

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1673

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.4.2.20					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1674
Out-of-	02-Oct-2024	9.1	A vulnerability in the web-	https://sec.clou	O-CIS-RV04-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/1675
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to	https://sec.clou dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1676

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1677
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV04-211024/1678

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1679

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1680

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20517		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1681
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 1.4.2.22					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1683

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1684
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1686

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1687
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1690
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV04-211024/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 1.5.1.05					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1693
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1694

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1695

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1696
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1698

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1699

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20516		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1700
Affected Version(s): 1.5.1.11					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1701

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1702

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1703
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1706
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1709
Affected Version(s): 1.5.1.13					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1711

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1712
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1713

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1714

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1715
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1717

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1718

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20524		
Affected Version(s): 3.0.0.1-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1719
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1721

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1722
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1723

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1725
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 3.0.0.19-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1728
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1731
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1732

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1734
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1736

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 3.0.2.01-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1737
Out-of-	02-Oct-2024	9.1	A vulnerability in the web-	https://sec.clou	O-CIS-RV04-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/1738
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to	https://sec.clou dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1739

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1740
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV04-211024/1741

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1742

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1743

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20524		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1744
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 4.0.0.7					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1746

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1747
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1749

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1750
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1753
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV04-211024/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 4.0.2.08-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1755

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1756
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1757

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1758

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1759
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1761

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1762

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20517		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1763
Affected Version(s): 4.0.3.03-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1765

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1766
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1767

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1769
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1772
Affected Version(s): 4.0.4.02-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1773

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1774

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1775
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1776

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1777

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1778
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1780

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1781

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20516		
Affected Version(s): 4.1.0.02-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1782
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1784

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1785
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1786

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1788
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 4.1.1.01					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1791
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1793

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1794
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1795

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1797
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1799

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 4.2.1.02					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1800
Out-of-	02-Oct-2024	9.1	A vulnerability in the web-	https://sec.clou	O-CIS-RV04-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/1801
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to	https://sec.clou dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1802

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1803
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV04-211024/1804

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1805

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1806

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20516		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1807
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 4.2.2.08					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1809

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1810
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1812

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1813
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1815

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1816
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV04-211024/1817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 4.2.3.03					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1818

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1819
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1820

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1821

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1822
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1824

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1825

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20517		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1826
Affected Version(s): 4.2.3.06					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1827

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1829
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1832
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1834

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1835
Affected Version(s): 4.2.3.07					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1837

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1838
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1839

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1840

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1841
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1843

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1844

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20524		
Affected Version(s): 4.2.3.08					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1845
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1847

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1848
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1849

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1851
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1853

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 4.2.3.09					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1854
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1857
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1858

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1860
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1862

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 4.2.3.10					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1863
Out-of-	02-Oct-2024	9.1	A vulnerability in the web-	https://sec.clou	O-CIS-RV04-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/1864
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to	https://sec.clou dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1865

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1866
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV04-211024/1867

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1868

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1869

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20524		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1870
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 4.2.3.14					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1872

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1873
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1875

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1876
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1879
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV04-211024/1880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	rv04x_rv32x_vulns-yJ2OSDhV	
Product: rv042_firmware					
Affected Version(s): 1.0.1.17					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1881

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1882
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV04-211024/1883

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1884

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1885
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV04-211024/1886

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1887

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1889
Affected Version(s): 1.0.2.03					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1890

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1891

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1892
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1895
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1898
Affected Version(s): 1.1.0.09					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV04-211024/1899

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1900

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1901
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vul	O-CIS-RV04-211024/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	ns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1903

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1904
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV04-211024/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1906

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1907

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20517		
Affected Version(s): 1.1.1.06					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1908
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1910

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1911
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1912

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1913

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1914
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1916

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 1.1.1.19					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1917
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1919

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1920
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1921

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1923
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1924

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1925

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.2.1.13					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1926
Out-of-	02-Oct-2024	9.1	A vulnerability in the web-	https://sec.clou	O-CIS-RV04-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/1927
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1928

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1929
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV04-211024/1930

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1931

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1932

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20517		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1933
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 1.2.1.14					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1935

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1936
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1938

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1939
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1941

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1942
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV04-211024/1943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 1.3.1.10					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1944

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1945
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1946

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1948
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1950

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1951

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20516		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1952
Affected Version(s): 1.3.1.12					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1953

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1954

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1955
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1956

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1958
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1961
Affected Version(s): 1.3.12.19-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1962

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1964
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1965

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1966

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1967
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1969

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1970

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20524		
Affected Version(s): 1.3.12.6-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1971
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1973

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1974
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1975

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1977
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1978

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.3.13.02-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1980
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1983
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1984

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1986
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/1987

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1988

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 1.3.2.02					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1989
Out-of-	02-Oct-2024	9.1	A vulnerability in the web-	https://sec.clou	O-CIS-RV04-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/1990
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to	https://sec.clou dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1991

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1992
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV04-211024/1993

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1994

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1995

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20524		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1996
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.4.2.15					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1998

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/1999
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2001

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2002
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2004

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2005
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV04-211024/2006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 1.4.2.17					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2007

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2008
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2009

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2010

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2011
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2012

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2013

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2014

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20516		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2015
Affected Version(s): 1.4.2.19					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2017

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2018
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2019

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2021
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2024
Affected Version(s): 1.4.2.20					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2025

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2026

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2027
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2028

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2029

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2030
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2032

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2033

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20517		
Affected Version(s): 1.4.2.22					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2034
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2036

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2037
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2038

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2040
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2041

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 1.5.1.05					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2043
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2046
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2047

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2049
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2051

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.5.1.11					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2052
Out-of-	02-Oct-2024	9.1	A vulnerability in the web-	https://sec.clou	O-CIS-RV04-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2053
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to	https://sec.clou dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2054

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2055
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV04-211024/2056

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2057

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2058

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20517		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2059
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 1.5.1.13					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2061

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2062
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2063

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2064

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2065
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2067

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2068
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV04-211024/2069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 3.0.0.1-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2070

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2071
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2072

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2073

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2074
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2076

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2077

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20516		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2078
Affected Version(s): 3.0.0.19-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2079

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2080

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2081
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2082

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2084
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2086

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2087
Affected Version(s): 3.0.2.01-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2088

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2089

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2090
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2091

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2092

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2093
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2095

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2096

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20524		
Affected Version(s): 4.0.0.7					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2097
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2099

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2100
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2101

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2103
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 4.0.2.08-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2106
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2109
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2110

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2112
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2113

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2114

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 4.0.3.03-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2115
Out-of-	02-Oct-2024	9.1	A vulnerability in the web-	https://sec.clou	O-CIS-RV04-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2116
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to	https://sec.clou dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2117

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2118
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV04-211024/2119

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2120

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2121

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20524		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2122
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 4.0.4.02-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2124

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2125
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2126

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2127

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2128
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2130

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2131
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV04-211024/2132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 4.1.0.02-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2133

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2134
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2135

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2136

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2137
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2139

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2140

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20516		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2141
Affected Version(s): 4.1.1.01					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2142

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2143

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2144
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2145

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2147
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2148

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2149

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2150
Affected Version(s): 4.2.1.02					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2151

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2152

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2153
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2154

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2155

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2156
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2157

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2158

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2159

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20517		
Affected Version(s): 4.2.2.08					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2160
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2162

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2163
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2164

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2166
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2167

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2168

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 4.2.3.03					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2169
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2171

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2172
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2173

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2175
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2177

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 4.2.3.06					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2178
Out-of-	02-Oct-2024	9.1	A vulnerability in the web-	https://sec.clou	O-CIS-RV04-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2179
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2180

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2181
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV04-211024/2182

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2183

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2184

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20517		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2185
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 4.2.3.07					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2187

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2188
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2189

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2190

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2191
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2192

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2194
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV04-211024/2195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 4.2.3.08					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2196

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2197
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2198

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2200
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2202

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2203

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20516		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2204
Affected Version(s): 4.2.3.09					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2205

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2206

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2207
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2208

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2210
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2213
Affected Version(s): 4.2.3.10					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2215

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2216
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2217

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2218

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2219
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV04-211024/2220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2221

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2222

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20524		
Affected Version(s): 4.2.3.14					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2223
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2225

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2226
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2227

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2229
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2230

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV04-211024/2231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Product: rv320_firmware					
Affected Version(s): 1.0.1.17					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2232
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2233

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2234

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2235
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2236

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2238
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2240

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 1.0.2.03					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2241

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20521		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2242
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2243

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2244
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2245
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2246

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2247

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2248
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.1.0.09					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2250

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2251
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2252

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2253

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2254
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2257
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 1.1.1.06					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2259

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2260
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2262

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2263
Out-of-bounds	02-Oct-2024	6.8	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2265

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2267
Affected Version(s): 1.1.1.19					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2268

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2269

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2270
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2272

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2273
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2275

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2276
Affected Version(s): 1.2.1.13					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2277

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2278

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2279
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2280

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2281

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2282
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2284

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.2.1.14					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2286
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2287

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2288

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20519		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2289
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2290

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2291

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2292
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2294

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 1.3.1.10					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2295
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2297

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2298
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2299

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2300

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2301
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2303

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.3.1.12					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2304

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20521		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2305
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2306

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2307
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2308
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2309

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2311
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 1.3.12.19-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2313

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2314
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2315

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2316

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2317
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2320
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 1.3.12.6-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2322

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2323
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2325

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2326
Out-of-bounds	02-Oct-2024	6.8	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2328

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2330
Affected Version(s): 1.3.13.02-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2331

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2332

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2333
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2335

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2336
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2338

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2339
Affected Version(s): 1.3.2.02					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2340

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2341

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2342
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2345
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2347

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 1.4.2.15					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2349
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2351

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20518		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2352
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2353

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2355
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2357

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.4.2.17					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2358
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2360

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2361
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2362

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2364
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2366

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 1.4.2.19					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2367

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20521		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2368
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2369

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2370
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2371
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2372

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2373

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2374
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.4.2.20					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2376

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2377
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2378

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2380
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2383
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 1.4.2.22					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2385

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2386
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2388

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2389
Out-of-bounds	02-Oct-2024	6.8	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2391

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2393
Affected Version(s): 1.5.1.05					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2394

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2395

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2396
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2398

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2399
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2401

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2402
Affected Version(s): 1.5.1.11					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2403

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2404

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2405
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2406

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2407

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2408
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2410

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.5.1.13					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2412
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2414

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20520		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2415
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2416

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2418
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2420

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 3.0.0.1-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2421
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2422

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2423

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2424
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2425

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2427
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2429

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 3.0.0.19-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2430

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20521		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2431
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2432

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2433
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2434
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2435

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2437
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 3.0.2.01-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2439

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2440
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2442

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2443
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2446
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 4.0.0.7					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2448

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2449
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2451

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2452
Out-of-bounds	02-Oct-2024	6.8	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2454

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2456
Affected Version(s): 4.0.2.08-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2457

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2458

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2459
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2461

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2462
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2464

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2465
Affected Version(s): 4.0.3.03-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2467

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2468
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2470

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2471
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2473

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 4.0.4.02-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2475
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2476

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2477

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20519		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2478
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2479

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2480

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2481
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2483

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 4.1.0.02-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2484
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2486

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2487
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2488

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2490
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2492

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 4.1.1.01					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2493

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20520		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2494
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2495

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2496
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2497
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2498

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2499

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2500
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 4.2.1.02					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2503
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2504

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2505

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2506
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2509
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 4.2.2.08					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2511

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2512
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2513

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2514

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2515
Out-of-bounds	02-Oct-2024	6.8	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2517

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2519
Affected Version(s): 4.2.3.03					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2520

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2521

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2522
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2524

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2525
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2527

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2528
Affected Version(s): 4.2.3.06					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2529

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2530

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2531
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2532

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2533

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2534
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2536

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2537

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 4.2.3.07					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2538
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2539

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2540

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20518		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2541
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2542

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2544
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2546

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 4.2.3.08					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2547
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2548

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2549

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2550
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2551

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2553
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2555

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 4.2.3.09					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2556

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20521		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2557
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2558

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2559
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2560
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2561

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2562

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2563
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 4.2.3.10					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2565

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2566
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2568

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2569
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2572
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 4.2.3.14					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2574

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2575
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2577

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2578
Out-of-bounds	02-Oct-2024	6.8	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2580

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2582
Product: rv325_firmware					
Affected Version(s): 1.0.1.17					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2583

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2585
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2586

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2587

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2588
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2590

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2591
Affected Version(s): 1.0.2.03					
Out-of-	02-Oct-2024	9.1	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2592
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to	https://sec.clou dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2593

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2594
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV32-211024/2595

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	ecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2596

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2597
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2598
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2599

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 1.1.0.09					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2601
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2603

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2604
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2605

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2606

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2607
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.1.1.06					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2610
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV32-211024/2611

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2612

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2613
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2614

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2615

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2616
Out-of-bounds	02-Oct-2024	6.8	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2618

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 1.1.1.19					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2619

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20520		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2620
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2621

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2622
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2623
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2624

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2626
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Affected Version(s): 1.2.1.13					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2628

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2629
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2632
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2634

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2635
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 1.2.1.14					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2637

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2638
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2639

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2640

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2641
Out-of-bounds	02-Oct-2024	6.8	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2643

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2645
Affected Version(s): 1.3.1.10					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2646

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2647

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2648
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2650

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2651
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2653

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2654
Affected Version(s): 1.3.1.12					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2655

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2656

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2657
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2658

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2660
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2662

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 1.3.12.19-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2664
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2665

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2666

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20518		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2667
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2668

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2670
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2672

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 1.3.12.6-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2673
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2674

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2675

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2676
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2677

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2679
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2681

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 1.3.13.02-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2682

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20521		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2683
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2684

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2685
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2686
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2687

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2688

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2689
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 1.3.2.02					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2691

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2692
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2693

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2694

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2695
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2698
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 1.4.2.15					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2700

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2701
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2702

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2703

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2704
Out-of-bounds	02-Oct-2024	6.8	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2706

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2708
Affected Version(s): 1.4.2.17					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2709

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2710

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2711
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2713

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2714
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2716

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2717
Affected Version(s): 1.4.2.19					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2718

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2719

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2720
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2721

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2722

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2723
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2725

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 1.4.2.20					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2727
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2729

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20519		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2730
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2731

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2732

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2733
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2735

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 1.4.2.22					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2736
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2737

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2738

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2739
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2740

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2742
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2744

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Affected Version(s): 1.5.1.05					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2745

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20520		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2746
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2747

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2748
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2749
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2750

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2752
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 1.5.1.11					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2754

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2755
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2756

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2757

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2758
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2761
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 1.5.1.13					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2763

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2764
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2765

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2766

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2767
Out-of-bounds	02-Oct-2024	6.8	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2769

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2771
Affected Version(s): 3.0.0.1-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2772

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2773

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2774
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2776

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2777
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2779

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2780
Affected Version(s): 3.0.0.19-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2782

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2783
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2785

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2786
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2788

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 3.0.2.01-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2790
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2792

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20518		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2793
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2794

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2796
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2798

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 4.0.0.7					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2799
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2801

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2802
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2803

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2805
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2807

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 4.0.2.08-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2808

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20520		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2809
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2810

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2811
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2812
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2813

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2815
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 4.0.3.03-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2817

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2818
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2819

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2821
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2824
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 4.0.4.02-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2826

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2827
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2829

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2830
Out-of-bounds	02-Oct-2024	6.8	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2832

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2833

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2834
Affected Version(s): 4.1.0.02-tm					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2835

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2836

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2837
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2839

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2840
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2842

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2843
Affected Version(s): 4.1.1.01					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2844

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2845

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2846
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2847

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2848

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2849
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2851

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2852

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 4.2.1.02					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2853
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2854

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2855

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20519		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2856
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2857

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2859
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2861

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 4.2.2.08					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2862
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2864

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2865
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2866

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2868
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2870

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 4.2.3.03					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2871

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20521		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2872
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2873

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2874
Out-of-	02-Oct-2024	6.8	A vulnerability in the web-	https://sec.clou	O-CIS-RV32-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Write			based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	211024/2875
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2876

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2878
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 4.2.3.06					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2880

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2881
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2882

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2883

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2884
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2886

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2887
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Affected Version(s): 4.2.3.07					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. 	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2889

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2890
Out-of-bounds	02-Oct-2024	9.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2892

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2893
Out-of-bounds	02-Oct-2024	6.8	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV32-211024/2894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2895

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2897
Affected Version(s): 4.2.3.08					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2898

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2899

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2900
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2902

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2903
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2905

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2906
Affected Version(s): 4.2.3.09					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2907

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2908

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2909
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2910

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2911

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2912
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2913

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2914

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID: CVE-2024-20516**		
Affected Version(s): 4.2.3.10					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2916
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2917

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2918

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20518		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2919
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2920

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2922
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2924

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**		
Affected Version(s): 4.2.3.14					
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20521**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2925
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV32-211024/2926

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20520**	rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2927

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20519**		
Out-of-bounds Write	02-Oct-2024	9.1	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID: CVE-2024-20518**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2928
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2929

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20517**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20522**		
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20524**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2931
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV32-211024/2932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20523**	/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	
Out-of-bounds Write	02-Oct-2024	6.8	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV	O-CIS-RV32-211024/2933

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			  This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. **CVE ID: CVE-2024-20516**		
Product: rv340w_dual_wan_gigabit_wireless-ac_vpn_router_firmware					
Affected Version(s): 1.0.00.29					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2934
N/A	02-Oct-2024	7.2	A vulnerability in the web-	https://sec.clou	O-CIS-RV34-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	211024/2935
Affected Version(s): 1.0.00.33					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2936

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2937
Affected Version(s): 1.0.01.16					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-	O-CIS-RV34-211024/2938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	privesc-rce-qE33TCms	
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2939

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.01.17					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2940
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2941

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.01.18					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2942
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV34-211024/2943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	ecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	
Affected Version(s): 1.0.01.20					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2944

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2945
Affected Version(s): 1.0.02.16					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2946

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2947

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20470		
Affected Version(s): 1.0.03.15					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2948
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2949

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.16					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2950
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-	O-CIS-RV34-211024/2951

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	qE33TCms	
Affected Version(s): 1.0.03.17					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2952

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2953
Affected Version(s): 1.0.03.18					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2954

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2955
Affected Version(s): 1.0.03.19					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2956
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2957

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.20					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2958
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2959

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.21					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2960

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20393		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2961
Affected Version(s): 1.0.03.22					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2962

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2963
Affected Version(s): 1.0.03.24					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV34-211024/2964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2965

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.26					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2966
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.27					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2968
N/A	02-Oct-2024	7.2	A vulnerability in the web-	https://sec.clou	O-CIS-RV34-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	211024/2969
Affected Version(s): 1.0.03.28					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2970

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2971
Affected Version(s): 1.0.03.29					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-	O-CIS-RV34-211024/2972

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	privesc-rce-qE33TCms	
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2973

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Product: rv340_dual_wan_gigabit_vpn_router_firmware					
Affected Version(s): 1.0.00.29					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2974
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2975

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.00.33					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2976
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV34-211024/2977

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	
Affected Version(s): 1.0.01.16					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2979
Affected Version(s): 1.0.01.17					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-	O-CIS-RV34-211024/2980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	qE33TCms	
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2981

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.01.18					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2982
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2983

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.01.20					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2984
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV34-211024/2985

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	/cisco-sa-rv34x-privesc-rce-qE33TCms	
Affected Version(s): 1.0.02.16					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2986

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2987
Affected Version(s): 1.0.03.15					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2988

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2989

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20470		
Affected Version(s): 1.0.03.16					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2990
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2991

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.17					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2992
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-	O-CIS-RV34-211024/2993

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	qE33TCms	
Affected Version(s): 1.0.03.18					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2994

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2995
Affected Version(s): 1.0.03.19					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2996

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2997
Affected Version(s): 1.0.03.20					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2998
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/2999

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.21					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3000
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3001

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.22					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3002

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20393		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3003
Affected Version(s): 1.0.03.24					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3004

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3005
Affected Version(s): 1.0.03.26					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV34-211024/3006

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3007

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.27					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3008
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3009

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.28					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3010
N/A	02-Oct-2024	7.2	A vulnerability in the web-	https://sec.clou	O-CIS-RV34-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	211024/3011
Affected Version(s): 1.0.03.29					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3012

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3013
Product: rv345p_dual_wan_gigabit_poe_vpn_router_firmware					
Affected Version(s): 1.0.00.29					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV34-211024/3014

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	ecurityAdvisory /cisco-sa-rv34x-privesc-rce-qE33TCms	
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3015

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.00.33					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3016
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3017

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.01.16					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3018
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV34-211024/3019

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	
Affected Version(s): 1.0.01.17					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3020

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3021
Affected Version(s): 1.0.01.18					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-	O-CIS-RV34-211024/3022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	qE33TCms	
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3023

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.01.20					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3024
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3025

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.02.16					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3026
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV34-211024/3027

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	/cisco-sa-rv34x-privesc-rce-qE33TCms	
Affected Version(s): 1.0.03.15					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3028

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3029
Affected Version(s): 1.0.03.16					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3030

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3031

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20470		
Affected Version(s): 1.0.03.17					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3032
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3033

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.18					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3034
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-	O-CIS-RV34-211024/3035

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	qE33TCms	
Affected Version(s): 1.0.03.19					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3036

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3037
Affected Version(s): 1.0.03.20					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3038

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3039
Affected Version(s): 1.0.03.21					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3040
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3041

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.22					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3042
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3043

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.24					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3044

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20393		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3045
Affected Version(s): 1.0.03.26					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3046

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3047
Affected Version(s): 1.0.03.27					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV34-211024/3048

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3049

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.28					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3050
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3051

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.29					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3052
N/A	02-Oct-2024	7.2	A vulnerability in the web-	https://sec.clou	O-CIS-RV34-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	dapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	211024/3053
Product: rv345_dual_wan_gigabit_vpn_router_firmware					
Affected Version(s): 1.0.00.29					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based	https://sec.clouddapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3054

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3055
Affected Version(s): 1.0.00.33					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W,	https://sec.cloudapps.cisco.com/security/center/content/CiscoS	O-CIS-RV34-211024/3056

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	ecurityAdvisory /cisco-sa-rv34x-privesc-rce-qE33TCms	
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3057

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.01.16					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3058
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3059

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.01.17					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3060
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com	O-CIS-RV34-211024/3061

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	
Affected Version(s): 1.0.01.18					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3063
Affected Version(s): 1.0.01.20					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-	O-CIS-RV34-211024/3064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	qE33TCms	
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3065

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.02.16					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3066
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3067

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.15					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3068
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV34-211024/3069

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	/cisco-sa-rv34x-privesc-rce-qE33TCms	
Affected Version(s): 1.0.03.16					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3070

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3071
Affected Version(s): 1.0.03.17					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3072

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3073

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20470		
Affected Version(s): 1.0.03.18					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3074
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3075

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.19					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3076
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-	O-CIS-RV34-211024/3077

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	qE33TCms	
Affected Version(s): 1.0.03.20					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3078

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3079
Affected Version(s): 1.0.03.21					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3080

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3081
Affected Version(s): 1.0.03.22					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3082
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3083

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.24					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3084
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3085

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.26					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3086

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20393		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3087
Affected Version(s): 1.0.03.27					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3088

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**		
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3089
Affected Version(s): 1.0.03.28					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small	https://sec.cloudapps.cisco.com/security/center	O-CIS-RV34-211024/3090

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3091

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Affected Version(s): 1.0.03.29					
N/A	02-Oct-2024	8.8	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin. **CVE ID: CVE-2024-20393**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3092
N/A	02-Oct-2024	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms	O-CIS-RV34-211024/3093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. **CVE ID: CVE-2024-20470**		
Vendor: Dlink					
Product: dir-605l_firmware					
Affected Version(s): 2.13b01					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. Affected is the function formEasySetPassword of the file /goform/formEasySetPassword. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9534**	N/A	O-DLI-DIR--211024/3094
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been rated as critical. Affected by this issue is the function formSetWanNonLogin of the file /goform/formSetWanNonLogin. The manipulation of the argument webpage	N/A	O-DLI-DIR--211024/3095

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9552**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Oct-2024	8.8	A vulnerability has been found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This vulnerability affects the function formAdvanceSetup of the file /goform/formAdvanceSetup. The manipulation of the argument webpage leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9532**	N/A	O-DLI-DIR--211024/3096
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability classified as critical has been found in D-Link DIR-605L 2.13B01 BETA. This affects the function formdumpeasysetup of the file /goform/formdumpeasysetup. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9553**	N/A	O-DLI-DIR--211024/3097
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability, which was classified as critical, has been found in D-Link DIR-605L 2.13B01 BETA. Affected by this issue is the function formSetEasy_Wizard of the file /goform/formSetEasy_Wizard. The manipulation of the	N/A	O-DLI-DIR--211024/3098

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument curTime leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9555**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability, which was classified as critical, was found in D-Link DIR-605L 2.13B01 BETA. This affects the function formSetEnableWizard of the file /goform/formSetEnableWizard. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9556**	N/A	O-DLI-DIR--211024/3099
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability has been found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This vulnerability affects the function formSetWanPPPoE of the file /goform/formSetWanPPPoE. The manipulation of the argument webpage leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9557**	N/A	O-DLI-DIR--211024/3100
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This issue affects the function formDeviceReboot of the file /goform/formDeviceReboot. The manipulation of the	N/A	O-DLI-DIR--211024/3101

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument next_page leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9533**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability has been found in D-Link DIR-605L 2.13B01 BETA and classified as critical. Affected by this vulnerability is the function formSetPassword of the file /goform/formSetPassword. The manipulation of the argument curTime leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9565**	N/A	O-DLI-DIR--211024/3102
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability, which was classified as critical, was found in D-Link DIR-605L 2.13B01 BETA. Affected is the function formWlanWizardSetup of the file /goform/formWlanWizardSetup. The manipulation of the argument webpage leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9564**	N/A	O-DLI-DIR--211024/3103
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability, which was classified as critical, has been found in D-Link DIR-605L 2.13B01 BETA. This issue affects the function formWlanSetup_Wizard of the file /goform/formWlanSetup_Wizard. The manipulation	N/A	O-DLI-DIR--211024/3104

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument webpage leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9563**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability classified as critical was found in D-Link DIR-605L 2.13B01 BETA. This vulnerability affects the function formSetWizard1/formSetWizard2. The manipulation of the argument curTime leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9562**	N/A	O-DLI-DIR--211024/3105
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability classified as critical has been found in D-Link DIR-605L 2.13B01 BETA. This affects the function formSetWAN_Wizard51/formSetWAN_Wizard52. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9561**	N/A	O-DLI-DIR--211024/3106
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. Affected is the function formWlanSetup of the file /goform/formWlanSetup. The manipulation of the argument webpage leads to buffer overflow. It is possible to launch the attack remotely. The exploit	N/A	O-DLI-DIR--211024/3107

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. **CVE ID: CVE-2024-9559**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This issue affects the function formSetWanPPTP of the file /goform/formSetWanPPTP. The manipulation of the argument webpage leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9558**	N/A	O-DLI-DIR--211024/3108
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been declared as critical. Affected by this vulnerability is the function formSetWanL2TP of the file /goform/formSetWanL2TP. The manipulation of the argument webpage leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9551**	N/A	O-DLI-DIR--211024/3109
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been declared as critical. This vulnerability affects the function formSetDomainFilter of the file /goform/formSetDomainFilter. The manipulation of the argument curTime leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	N/A	O-DLI-DIR--211024/3110

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-9514		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. This affects the function formSetQoS of the file /goform/formSetQoS. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9515**	N/A	O-DLI-DIR--211024/3111
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. Affected is the function formLogDnsquery of the file /goform/formLogDnsquery. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9550**	N/A	O-DLI-DIR--211024/3112
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This issue affects the function formEasySetupWizard/formEasySetupWizard2 of the file /goform/formEasySetupWizard. The manipulation of the argument curTime leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9549**	N/A	O-DLI-DIR--211024/3113

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Oct-2024	8.8	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been declared as critical. Affected by this vulnerability is the function formEasySetupWWConfig of the file /goform/formEasySetupWWConfig. The manipulation of the argument curTime leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9535**	N/A	O-DLI-DIR--211024/3114
Product: dir-619l_firmware					
Affected Version(s): 2.06b1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability was found in D-Link DIR-619L B1 2.06 and classified as critical. Affected by this issue is the function formEasySetTimezone of the file /goform/formEasySetTimezone. The manipulation of the argument curTime leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9570**	N/A	O-DLI-DIR--211024/3115
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability has been found in D-Link DIR-619L B1 2.06 and classified as critical. Affected by this vulnerability is the function formEasySetPassword of the file /goform/formEasySetPassword. The manipulation of the argument curTime leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public	N/A	O-DLI-DIR--211024/3116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and may be used. **CVE ID: CVE-2024-9569**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability, which was classified as critical, was found in D-Link DIR-619L B1 2.06. Affected is the function formAdvNetwork of the file /goform/formAdvNetwork. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9568**	N/A	O-DLI-DIR--211024/3117
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability, which was classified as critical, has been found in D-Link DIR-619L B1 2.06. This issue affects the function formAdvFirewall of the file /goform/formAdvFirewall. The manipulation of the argument curTime leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9567**	N/A	O-DLI-DIR--211024/3118
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2024	8.8	A vulnerability classified as critical was found in D-Link DIR-619L B1 2.06. This vulnerability affects the function formDeviceReboot of the file /goform/formDeviceReboot. The manipulation of the argument next_page leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-9566**	N/A	O-DLI-DIR--211024/3119

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Draytek					
Product: vigor1000b_firmware					
Affected Version(s): * Up to (excluding) 4.3.2.8					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3120
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3121
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3122
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3123
Affected Version(s): From (including) 4.4.0.0 Up to (excluding) 4.4.3.1					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the	N/A	O-DRA-VIGO-211024/3124

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3125
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3126
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3127
Product: vigor165_firmware					
Affected Version(s): * Up to (excluding) 4.2.7					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow.	N/A	O-DRA-VIGO-211024/3128

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41593		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3129
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3130
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3131
Product: vigor166_firmware					
Affected Version(s): * Up to (excluding) 4.2.7					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3132
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of	N/A	O-DRA-VIGO-211024/3133

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3134
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3135
Product: vigor2133_firmware					
Affected Version(s): *					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3136
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3137
Improper	03-Oct-2024	6.1	DrayTek Vigor3910 devices	N/A	O-DRA-VIGO-

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**		211024/3138
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3139
Product: vigor2135_firmware					
Affected Version(s): * Up to (excluding) 4.4.5.3					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3140
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3141
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3142

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3143
Product: vigor2620_firmware					
Affected Version(s): *					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3144
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3145
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3146
Improper Neutralization of Input During Web Page Generation ('Cross-site	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6.	N/A	O-DRA-VIGO-211024/3147

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID: CVE-2024-41587**		
Product: vigor2762_firmware					
Affected Version(s): *					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3148
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3149
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3150
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3151
Product: vigor2763_firmware					
Affected Version(s): * Up to (excluding) 4.4.5.3					
Out-of-bounds	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a	N/A	O-DRA-VIGO-211024/3152

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3153
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3154
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3155
Product: vigor2765_firmware					
Affected Version(s): * Up to (excluding) 4.4.5.3					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a	N/A	O-DRA-VIGO-211024/3156

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3157
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3158
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3159
Product: vigor2766_firmware					
Affected Version(s): * Up to (excluding) 4.4.5.3					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3160
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to	N/A	O-DRA-VIGO-211024/3161

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3162
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3163
Product: vigor2832_firmware					
Affected Version(s): *					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3164
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL.	N/A	O-DRA-VIGO-211024/3165

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41594		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3166
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3167
Product: vigor2860_firmware					
Affected Version(s): *					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3168
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3169
Improper Neutralization of Input During Web Page	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS.	N/A	O-DRA-VIGO-211024/3170

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			**CVE ID: CVE-2024-41591**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3171
Product: vigor2862_firmware					
Affected Version(s): *					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3172
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3173
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3174
Improper Neutralization of Input During Web	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting	N/A	O-DRA-VIGO-211024/3175

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**		
Product: vigor2865_firmware					
Affected Version(s): * Up to (excluding) 4.4.5.2					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3176
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3177
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3178
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3179
Product: vigor2866_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.4.5.2					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3180
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3181
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3182
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3183
Product: vigor2915_firmware					
Affected Version(s): * Up to (excluding) 4.4.5.3					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(),	N/A	O-DRA-VIGO-211024/3184

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3185
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3186
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3187
Product: vigor2925_firmware					
Affected Version(s): *					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow.	N/A	O-DRA-VIGO-211024/3188

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41593		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3189
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3190
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3191
Product: vigor2926_firmware					
Affected Version(s): *					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3192
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of	N/A	O-DRA-VIGO-211024/3193

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3194
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3195
Product: vigor2952_firmware					
Affected Version(s): *					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3196
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3197
Improper	03-Oct-2024	6.1	DrayTek Vigor3910 devices	N/A	O-DRA-VIGO-

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**		211024/3198
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3199
Product: vigor2962_firmware					
Affected Version(s): * Up to (excluding) 4.3.2.8					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3200
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3201
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3202

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3203
Affected Version(s): From (including) 4.4.0.0 Up to (excluding) 4.4.3.1					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3204
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3205
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3206
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6.	N/A	O-DRA-VIGO-211024/3207

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41587		
Product: vigor3220_firmware					
Affected Version(s): *					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3208
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3209
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3210
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3211
Product: vigor3910_firmware					
Affected Version(s): * Up to (excluding) 4.3.2.8					
Out-of-bounds	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a	N/A	O-DRA-VIGO-211024/3212

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Write			remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3213
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3214
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3215
Affected Version(s): From (including) 4.4.0.0 Up to (excluding) 4.4.3.1					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow.	N/A	O-DRA-VIGO-211024/3216

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41593		
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3217
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3218
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3219
Product: vigor3912_firmware					
Affected Version(s): * Up to (excluding) 4.3.6.1					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3220
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of	N/A	O-DRA-VIGO-211024/3221

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	6.1	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**	N/A	O-DRA-VIGO-211024/3222
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3223
Product: vigorlte200_firmware					
Affected Version(s): *					
Out-of-bounds Write	03-Oct-2024	9.8	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow. **CVE ID: CVE-2024-41593**	N/A	O-DRA-VIGO-211024/3224
Inadequate Encryption Strength	03-Oct-2024	7.5	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL. **CVE ID: CVE-2024-41594**	N/A	O-DRA-VIGO-211024/3225
Improper	03-Oct-2024	6.1	DrayTek Vigor3910 devices	N/A	O-DRA-VIGO-

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			through 4.3.2.6 allow unauthenticated DOM-based reflected XSS. **CVE ID: CVE-2024-41591**		211024/3226
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2024	5.4	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6. **CVE ID: CVE-2024-41587**	N/A	O-DRA-VIGO-211024/3227
Vendor: Google					
Product: android					
Affected Version(s): 12.0					
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699. **CVE ID: CVE-2024-20093**	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3228
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3229
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3230

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**		
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630. **CVE ID: CVE-2024-20097**	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3231
Out-of-bounds Read	07-Oct-2024	4.4	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701. **CVE ID: CVE-2024-20091**	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3232
Affected Version(s): 13.0					
Out-of-bounds Read	07-Oct-2024	4.9	In wlan driver, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998892; Issue ID: MSV-1601. **CVE ID: CVE-2024-20102**	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3233
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3234

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**		
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3235
Affected Version(s): 14.0					
Out-of-bounds Read	07-Oct-2024	4.9	In wlan driver, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998892; Issue ID: MSV-1601. **CVE ID: CVE-2024-20102**	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3236
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3237
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**		
Affected Version(s): 15.0					
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636. **CVE ID: CVE-2024-20095**	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3239
Out-of-bounds Read	07-Oct-2024	4.4	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635. **CVE ID: CVE-2024-20096**	https://corp.mediatek.com/product-security-bulletin/October-2024	O-GOO-ANDR-211024/3240
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	4.8	There is a reflected cross site scripting in Esri Portal for ArcGIS 11.1 and below on Windows and Linux x64 allows a remote authenticated attacker with administrative access to supply a crafted string which could potentially execute arbitrary JavaScript code in the their own browser (Self XSS). A user cannot be phished into clicking a link to execute code.	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	O-LIN-LINU-211024/3241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-25707		
Affected Version(s): * Up to (excluding) 6.10.9					
Integer Overflow or Wraparound	09-Oct-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid overflow from uint32_t to uint8_t [WHAT & HOW] dmub_rb_cmd's ramping_boundary has size of uint8_t and it is assigned 0xFFFF. Fix it by changing it to uint8_t with value of 0xFF. This fixes 2 INTEGER_OVERFLOW issues reported by Coverity. **CVE ID: CVE-2024-47661**	https://git.kernel.org/stable/c/30d1b783b6eeaf49d311a072c70d618d993d01ec, https://git.kernel.org/stable/c/d6b54900c564e35989cf6813e4071504fa0a90e0	O-LIN-LINU-211024/3242
Vendor: Microchip					
Product: timeprovider_4100_grandmaster_firmware					
Affected Version(s): From (including) 1.0 Up to (excluding) 2.4.7					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Oct-2024	8.8	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Microchip TimeProvider 4100 (Configuration modules) allows Command Injection.This issue affects TimeProvider 4100: from 1.0 before 2.4.7. **CVE ID: CVE-2024-9054**	https://www.microchip.com/en-us/solutions/technologies/embedded-security/how-to-report-potential-product-security-vulnerabilities/timeprovider-4100-grandmaster-rce-through-configuration-file	O-MIC-TIME-211024/3243
Improper Neutralization of Special Elements used in an	04-Oct-2024	6.5	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Microchip TimeProvider	https://www.microchip.com/en-us/solutions/technologies/embedded-	O-MIC-TIME-211024/3244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			4100 (Data plot modules) allows SQL Injection.This issue affects TimeProvider 4100: from 1.0 before 2.4.7. **CVE ID: CVE-2024-7801**	security/how-to-report-potential-product-security-vulnerabilities/timeprovider-4100-grandmaster-unathenticated-sql-injection	
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Out-of-bounds Write	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47410**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-MIC-WIND-211024/3245
Access of Uninitialized Pointer	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47411**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-MIC-WIND-211024/3246
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user.	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-MIC-WIND-211024/3247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47418**		
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47412**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-MIC-WIND-211024/3248
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47413**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-MIC-WIND-211024/3249
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47414**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-MIC-WIND-211024/3250
Use After Free	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-MIC-WIND-211024/3251

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47415**		
Integer Overflow or Wraparound	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47416**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-MIC-WIND-211024/3252
Out-of-bounds Write	09-Oct-2024	7.8	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47417**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-MIC-WIND-211024/3253
Out-of-bounds Read	09-Oct-2024	5.5	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47419**	https://helpx.adobe.com/security/products/animate/apsb24-76.html	O-MIC-WIND-211024/3254
Out-of-	09-Oct-2024	5.5	Animate versions 23.0.7,	https://helpx.ad	O-MIC-WIND-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Read			24.0.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-47420**	obe.com/security/products/animate/apsb24-76.html	211024/3255
Improper Check for Unusual or Exceptional Conditions	09-Oct-2024	5.5	A problem with a detection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices enables a user with Windows non-administrative privileges to disable the agent. This issue may be leveraged by malware to disable the Cortex XDR agent and then to perform malicious activity. **CVE ID: CVE-2024-9469**	https://security.paloaltonetworks.com/CVE-2024-9469	O-MIC-WIND-211024/3256
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-2024	4.8	There is a reflected cross site scripting in Esri Portal for ArcGIS 11.1 and below on Windows and Linux x64 allows a remote authenticated attacker with administrative access to supply a crafted string which could potentially execute arbitrary JavaScript code in the their own browser (Self XSS). A user cannot be phished into clicking a link to execute code. **CVE ID: CVE-2024-25707**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2024-update-2-released/	O-MIC-WIND-211024/3257
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.20796					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing	https://msrc.microsoft.com/upd	O-MIC-WIND-211024/3258

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability **CVE ID: CVE-2024-43573**	ate-guide/vulnerability/CVE-2024-43573	
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3259
Product: windows_10_1607					
Affected Version(s): * Up to (excluding) 10.0.14393.7428					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3260
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3261
Product: windows_10_1809					
Affected Version(s): * Up to (excluding) 10.0.17763.6414					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3262
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3263
Product: windows_10_21h2					
Affected Version(s): * Up to (excluding) 10.0.19044.5011					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3264
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code	https://msrc.microsoft.com/upd	O-MIC-WIND-211024/3265

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-43572**	ate-guide/vulnerability/CVE-2024-43572	
Affected Version(s): * Up to (excluding) 10.0.22000.3260					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3266
Product: windows_10_22h2					
Affected Version(s): * Up to (excluding) 10.0.19045.5011					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3267
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3268
Product: windows_11_21h2					
Affected Version(s): * Up to (excluding) 10.0.22000.3260					
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3269
Product: windows_11_22h2					
Affected Version(s): * Up to (excluding) 10.0.22621.4317					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3270
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3271

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows_11_22h3					
Affected Version(s): * Up to (excluding) 10.0.22631.4317					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3272
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3273
Product: windows_11_23h2					
Affected Version(s): * Up to (excluding) 10.0.22631.4317					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3274
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3275
Product: windows_11_24h2					
Affected Version(s): * Up to (excluding) 10.0.26100.2033					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3276
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3277
Product: windows_server_2008_sp2					
Affected Version(s): * Up to (excluding) 6.0.6003.22918					
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-211024/3278

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43572	guide/vulnerability/CVE-2024-43572	
Product: windows_server_2012					
Affected Version(s): * Up to (excluding) 6.2.9200.25118					
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3279
Product: windows_server_2012_r2					
Affected Version(s): * Up to (excluding) 6.3.9600.22221					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3280
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3281
Product: windows_server_2016					
Affected Version(s): * Up to (excluding) 10.0.14393.7428					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3282
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3283
Product: windows_server_2019					
Affected Version(s): * Up to (excluding) 10.0.17763.6414					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3284

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3285
Product: windows_server_2022					
Affected Version(s): * Up to (excluding) 10.0.20348..2762					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3286
Affected Version(s): * Up to (excluding) 10.0.20348.2762					
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3287
Product: windows_server_23h2					
Affected Version(s): * Up to (excluding) 10.0.25398.1189					
N/A	08-Oct-2024	8.1	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-43573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573	O-MIC-WIND-211024/3288
N/A	08-Oct-2024	7.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-43572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572	O-MIC-WIND-211024/3289
Vendor: Paloaltonetworks					
Product: pan-os					
Affected Version(s): From (including) 10.1.0 Up to (excluding) 10.1.11					
N/A	09-Oct-2024	4.7	A privilege escalation (PE) vulnerability in the XML API of Palo Alto Networks PAN-OS software enables an authenticated PAN-OS administrator with restricted privileges to use a compromised XML API key to perform actions as a	https://security.paloaltonetworks.com/CVE-2024-9471	O-PAL-PAN--211024/3290

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			higher privileged PAN-OS administrator. For example, an administrator with "Virtual system administrator (read-only)" access could use an XML API key of a "Virtual system administrator" to perform write operations on the virtual system configuration even though they should be limited to read-only operations. **CVE ID: CVE-2024-9471**		
Affected Version(s): From (including) 10.2.0 Up to (excluding) 10.2.8					
N/A	09-Oct-2024	4.7	A privilege escalation (PE) vulnerability in the XML API of Palo Alto Networks PAN-OS software enables an authenticated PAN-OS administrator with restricted privileges to use a compromised XML API key to perform actions as a higher privileged PAN-OS administrator. For example, an administrator with "Virtual system administrator (read-only)" access could use an XML API key of a "Virtual system administrator" to perform write operations on the virtual system configuration even though they should be limited to read-only operations. **CVE ID: CVE-2024-9471**	https://security.paloaltonetworks.com/CVE-2024-9471	O-PAL-PAN--211024/3291
Affected Version(s): From (including) 11.0.0 Up to (excluding) 11.0.3					
N/A	09-Oct-2024	4.7	A privilege escalation (PE) vulnerability in the XML API of Palo Alto Networks PAN-OS software enables an authenticated PAN-OS administrator with restricted privileges to use a compromised XML API key to perform actions as a	https://security.paloaltonetworks.com/CVE-2024-9471	O-PAL-PAN--211024/3292

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			higher privileged PAN-OS administrator. For example, an administrator with "Virtual system administrator (read-only)" access could use an XML API key of a "Virtual system administrator" to perform write operations on the virtual system configuration even though they should be limited to read-only operations. **CVE ID: CVE-2024-9471**		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 10.0.0					
N/A	09-Oct-2024	4.7	A privilege escalation (PE) vulnerability in the XML API of Palo Alto Networks PAN-OS software enables an authenticated PAN-OS administrator with restricted privileges to use a compromised XML API key to perform actions as a higher privileged PAN-OS administrator. For example, an administrator with "Virtual system administrator (read-only)" access could use an XML API key of a "Virtual system administrator" to perform write operations on the virtual system configuration even though they should be limited to read-only operations. **CVE ID: CVE-2024-9471**	https://security.paloaltonetworks.com/CVE-2024-9471	O-PAL-PAN--211024/3293
Vendor: Qualcomm					
Product: fastconnect_6700_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-FAST-211024/3294

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: fastconnect_6800_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-FAST-211024/3295
Product: fastconnect_6900_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-FAST-211024/3296
Product: fastconnect_7800_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-FAST-211024/3297
Product: qam8295p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-QAM8-211024/3298
Product: qca6174a_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-QCA6-211024/3299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: qca6391_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-QCA6-211024/3300
Product: qca6426_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-QCA6-211024/3301
Product: qca6436_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-QCA6-211024/3302
Product: qca6574au_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-QCA6-211024/3303
Product: qca6584au_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-QCA6-211024/3304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: qca6595au_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-QCA6-211024/3305
Product: qca6595_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-QCA6-211024/3306
Product: qca6688aq_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-QCA6-211024/3307
Product: qca6696_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-QCA6-211024/3308
Product: qca6698aq_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-QCA6-211024/3309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: qcs410_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-QCS4-211024/3310
Product: qcs610_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-QCS6-211024/3311
Product: qcs6490_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-QCS6-211024/3312
Product: sa4150p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SA41-211024/3313
Product: sa4155p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-SA41-211024/3314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: sa6145p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SA61-211024/3315
Product: sa6150p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SA61-211024/3316
Product: sa6155p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SA61-211024/3317
Product: sa8145p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SA81-211024/3318
Product: sa8150p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-SA81-211024/3319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: sa8155p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SA81-211024/3320
Product: sa8195p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SA81-211024/3321
Product: sa8295p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SA82-211024/3322
Product: sd660_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SD66-211024/3323
Product: sd865_5g_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-SD86-211024/3324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: sg4150p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SG41-211024/3325
Product: snapdragon_660_mobile_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SNAP-211024/3326
Product: snapdragon_680_4g_mobile_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SNAP-211024/3327
Product: snapdragon_685_4g_mobile_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SNAP-211024/3328
Product: snapdragon_865\+_5g_mobile_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-SNAP-211024/3329

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: snapdragon_865_5g_mobile_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SNAP-211024/3330
Product: snapdragon_870_5g_mobile_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SNAP-211024/3331
Product: snapdragon_888\+_5g_mobile_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SNAP-211024/3332
Product: snapdragon_888_5g_mobile_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SNAP-211024/3333
Product: snapdragon_8_gen_1_mobile_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-SNAP-211024/3334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: snapdragon_auto_5g_modem-rf_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SNAP-211024/3335
Product: snapdragon_auto_5g_modem-rf_gen_2_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SNAP-211024/3336
Product: snapdragon_x55_5g_modem-rf_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SNAP-211024/3337
Product: snapdragon_xr2_5g_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SNAP-211024/3338
Product: sw5100p_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-SW51-211024/3339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: sw5100_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SW51-211024/3340
Product: sxr2130_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-SXR2-211024/3341
Product: video_collaboration_vc1_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-VIDE-211024/3342
Product: video_collaboration_vc3_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-VIDE-211024/3343
Product: wcd9335_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-WCD9-211024/3344

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: wcd9341_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-WCD9-211024/3345
Product: wcd9370_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-WCD9-211024/3346
Product: wcd9375_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-WCD9-211024/3347
Product: wcd9380_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-WCD9-211024/3348
Product: wcd9385_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-WCD9-211024/3349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: wcn3950_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-WCN3-211024/3350
Product: wcn3980_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-WCN3-211024/3351
Product: wcn3988_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-WCN3-211024/3352
Product: wcn3990_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-WCN3-211024/3353
Product: wsa8810_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-	O-QUA-WSA8-211024/3354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: wsa8815_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-WSA8-211024/3355
Product: wsa8830_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-WSA8-211024/3356
Product: wsa8835_firmware					
Affected Version(s): -					
Use After Free	07-Oct-2024	7.8	Memory corruption while maintaining memory maps of HLOS memory. **CVE ID: CVE-2024-43047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	O-QUA-WSA8-211024/3357