



National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

01 - 15 Jan 2021

Vol. 08 No. 01

<https://nciipc.gov.in/>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Adobe					
photoshop					
Heap-based Buffer Overflow	13-Jan-21	6.8	Adobe Photoshop version 22.1 (and earlier) is affected by a heap buffer overflow vulnerability when handling a specially crafted font file. Successful exploitation could lead to arbitrary code execution. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21006	https://helpx.adobe.com/security/products/photoshop/psb21-01.html	A-ADO-PHOT-210121/1
incopy					
Uncontrolled Search Path Element	13-Jan-21	5.1	InCopy version 15.1.1 (and earlier) for Windows is affected by an uncontrolled search path 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-2021-21010	https://helpx.adobe.com/security/products/incopy/psb21-05.html	A-ADO-INCO-210121/2
captivate					
Uncontrolled Search Path Element	13-Jan-21	5.1	Adobe Captivate 2019 version 11.5.1.499 (and earlier) is affected by an	https://helpx.adobe.com/security/pr	A-ADO-CAPT-210121/3

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			uncontrolled search path element vulnerability that could lead to privilege escalation. An attacker with permissions to write to the file system could leverage this vulnerability to escalate privileges. CVE ID : CVE-2021-21011	oducts/captive/apsb21-06.html	
bridge					
Out-of-bounds Write	13-Jan-21	6.8	Adobe Bridge version 11.0 (and earlier) is affected by an out-of-bounds write vulnerability when parsing TTF files 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-2021-21012	https://helpx.adobe.com/security/products/bridge/apsb21-07.html	A-ADO-BRID-210121/4
Out-of-bounds Write	13-Jan-21	6.8	Adobe Bridge version 11.0 (and earlier) is affected by an out-of-bounds write vulnerability when parsing TTF files 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-2021-21013	https://helpx.adobe.com/security/products/bridge/apsb21-07.html	A-ADO-BRID-210121/5
animate					
Uncontrolled Search Path Element	13-Jan-21	6.8	Adobe Animate version 21.0 (and earlier) is affected by an uncontrolled search path	https://helpx.adobe.com/security/pr	A-ADO-ANIM-210121/6

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			element 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-2021-21008	oducts/animate/apsb21-03.html	
illustrator					
Uncontrolled Search Path Element	13-Jan-21	6.8	Adobe Illustrator version 25.0 (and earlier) is affected by an uncontrolled search path element 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-2021-21007	https://helpx.adobe.com/security/products/illustrator/apsb21-02.html	A-ADO-ILLU-210121/7
Cisco					
application_extension_platform					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	A-CIS-APPL-210121/8

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1146</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	A-CIS-APPL-210121/9

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1147</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1148</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	A-CIS-APPL-210121/10

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1149</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	A-CIS-APPL-210121/11
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-	A-CIS-APPL-210121/12

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1150</p>	inject-LBdQ2KRN	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	A-CIS-APPL-210121/13

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1151</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	A-CIS-APPL-210121/14

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1152</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1153</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	A-CIS-APPL-210121/15
Improper Neutralization of Input During Web Page Generation	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	A-CIS-APPL-210121/16

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			<p>authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1154</p>	sco-sa-rv-stored-xss-LPTQ3EQC	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	A-CIS-APPL-210121/17

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1155</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	A-CIS-APPL-210121/18

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have valid administrator credentials on the affected device. CVE ID : CVE-2021-1156		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1157	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	A-CIS-APPL-210121/19
Improper Neutralization of Input During Web Page Generation	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	A-CIS-APPL-210121/20

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			<p>authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1158</p>	sco-sa-rv-stored-xss-LPTQ3EQC	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	A-CIS-APPL-210121/21

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1159</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/22

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1160		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	A-CIS-APPL-210121/23

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1161</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/24

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1162</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/25

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1163		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1164	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	A-CIS-APPL-210121/26

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1165</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/27
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	A-CIS-APPL-210121/28

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1166</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	A-CIS-APPL-210121/29

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1167	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	A-CIS-APPL-210121/30

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1168</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	A-CIS-APPL-210121/31

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1169</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/32

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1170</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	A-CIS-APPL-210121/33

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1171</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/34

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1172</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/35

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1173		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1174	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	A-CIS-APPL-210121/36

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1175</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/37
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	A-CIS-APPL-210121/38

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1176</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	A-CIS-APPL-210121/39

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1177	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	A-CIS-APPL-210121/40

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1178</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	A-CIS-APPL-210121/41

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1184</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/42

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1185</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	A-CIS-APPL-210121/43

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1186</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/44

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1187</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/45

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1188		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1189	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	A-CIS-APPL-210121/46

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1192</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/47
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	A-CIS-APPL-210121/48

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1193</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-</p>	A-CIS-APPL-210121/49

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1194	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	A-CIS-APPL-210121/50

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1195</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	A-CIS-APPL-210121/51

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1196</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/52

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1197</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	A-CIS-APPL-210121/53

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1198</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/54

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1199</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/55

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1206		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1207	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	A-CIS-APPL-210121/56

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1208</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/57
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	A-CIS-APPL-210121/58

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1209</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	A-CIS-APPL-210121/59

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1210	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	A-CIS-APPL-210121/60

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1211</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	A-CIS-APPL-210121/61

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1212</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/62

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1213</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	A-CIS-APPL-210121/63

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1214</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/64

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1215</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	A-CIS-APPL-210121/65

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1216							
emergency_responder										
Insertion of Sensitive Information into Log File	13-Jan-21	4	A vulnerability in the audit logging component of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, Cisco Unity Connection, Cisco Emergency Responder, and Cisco Prime License Manager could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. The vulnerability is due to the storage of certain unencrypted credentials. An attacker could exploit this vulnerability by accessing the audit logs on an affected system and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage network devices. CVE ID : CVE-2021-1226	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-logging-6QSWKRYz	A-CIS-EMER-210121/66					
unified_communications_manager_im_&_presence_service										
Insertion of	13-Jan-21	4	A vulnerability in the audit	https://tools	A-CIS-UNIF-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information into Log File			<p>logging component of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, Cisco Unity Connection, Cisco Emergency Responder, and Cisco Prime License Manager could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. The vulnerability is due to the storage of certain unencrypted credentials. An attacker could exploit this vulnerability by accessing the audit logs on an affected system and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage network devices.</p> <p>CVE ID : CVE-2021-1226</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-logging-6QSWKRYz	210121/67

anyconnect_secure_mobility_client

Uncontrolled Search Path Element	13-Jan-21	7.2	<p>A vulnerability in the Network Access Manager and Web Security Agent components of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-	A-CIS-ANYC-210121/68
----------------------------------	-----------	-----	---	---	----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>injection attack. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of resources that are loaded by the application at run time. An attacker could exploit this vulnerability by inserting a configuration file in a specific path in the system which, in turn, causes a malicious DLL file to be loaded when the application starts. A successful exploit could allow the attacker to execute arbitrary code on the affected machine with SYSTEM privileges.</p> <p>CVE ID : CVE-2021-1237</p>	dll-injec-pQnryXLf	

unified_communications_manager

Insertion of Sensitive Information into Log File	13-Jan-21	4	<p>A vulnerability in the audit logging component of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, Cisco Unity Connection, Cisco Emergency Responder, and Cisco Prime License Manager could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. The</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-logging-6QSWKRYz</p>	A-CIS-UNIF-210121/69
--	-----------	---	---	--	----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is due to the storage of certain unencrypted credentials. An attacker could exploit this vulnerability by accessing the audit logs on an affected system and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage network devices.</p> <p>CVE ID : CVE-2021-1226</p>		
firepower_management_center					
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1223</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2</p>	A-CIS-FIRE-210121/70
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO)</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tcpfastopen-67DEwMe2</p>	A-CIS-FIRE-210121/71

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	er/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	
Always-Incorrect Control Flow Implementation	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	A-CIS-FIRE-210121/72

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>policies and deliver a malicious payload to the protected network.</p> <p>CVE ID : CVE-2021-1236</p>		
prime_license_manager					
Insertion of Sensitive Information into Log File	13-Jan-21	4	<p>A vulnerability in the audit logging component of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, Cisco Unity Connection, Cisco Emergency Responder, and Cisco Prime License Manager could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. The vulnerability is due to the storage of certain unencrypted credentials. An attacker could exploit this vulnerability by accessing the audit logs on an affected system and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage network devices.</p> <p>CVE ID : CVE-2021-1226</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-logging-6QSWKRYz</p>	A-CIS-PRIM-210121/73
enterprise_nfv_infrastructure_software					
Improper	13-Jan-21	3.5	A vulnerability in the web-	https://tools	A-CIS-ENTE-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			<p>based management interface of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. The vulnerability is due to improper input validation of log file content stored on the affected device. An attacker could exploit this vulnerability by modifying a log file with malicious code and getting a user to view the modified log file. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or to access sensitive, browser-based information.</p> <p>CVE ID : CVE-2021-1127</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-xss-smsz5Vhb	210121/74

firepower_threat_defense

Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	A-CIS-FIRE-210121/75
-------------------------------	-----------	---	---	---	----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1223		
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	A-CIS-FIRE-210121/76
Always-Incorrect Control Flow Implementation	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-	A-CIS-FIRE-210121/77

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network.</p> <p>CVE ID : CVE-2021-1236</p>	app-bypass-cSBYCATq	

unity_connection

Insertion of Sensitive Information into Log File	13-Jan-21	4	<p>A vulnerability in the audit logging component of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, Cisco Unity Connection, Cisco Emergency Responder, and Cisco Prime License Manager could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. The vulnerability is due to the storage of certain unencrypted credentials. An attacker could exploit this vulnerability by accessing the audit logs on an affected system and obtaining credentials that they may</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-logging-6QSWKRYz</p>	A-CIS-UNIT-210121/78
--	-----------	---	--	--	----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage network devices. CVE ID : CVE-2021-1226		
Concrete5					
concrete5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-21	3.5	The Express Entries Dashboard in Concrete5 8.5.4 allows stored XSS via the name field of a new data object at an index.php/dashboard/express/entries/view/ URI. CVE ID : CVE-2021-3111	https://documentation.concrete5.org/developers/introduction/version-history	A-CON-CONC-210121/79
courtbouillon					
cairosvg					
Uncontrolled Resource Consumption	06-Jan-21	4.3	CairoSVG is a Python (pypi) package. CairoSVG is an SVG converter based on Cairo. In CairoSVG before version 2.5.1, there is a regular expression denial of service (REDoS) vulnerability. When processing SVG files, the python package CairoSVG uses two regular expressions which are vulnerable to Regular Expression Denial of Service (REDoS). If an attacker provides a malicious SVG, it can make cairosvg get stuck processing the file for a very long time. This is fixed in version 2.5.1. See	https://github.com/Kozea/CairoSVG/commit/cfc9175e590531d90384aa88845052de53d94bf3 , https://github.com/Kozea/CairoSVG/security/advisories/GHSA-hq37-853p-g5cf	A-COU-CAIR-210121/80

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Referenced GitHub advisory for more information. CVE ID : CVE-2021-21236		
Elastic					
elasticsearch					
Insufficiently Protected Credentials	14-Jan-21	4	Elasticsearch versions 7.7.0 to 7.10.1 contain an information disclosure flaw in the async search API. Users who execute an async search will improperly store the HTTP headers. An Elasticsearch user with the ability to read the .tasks index could obtain sensitive request headers of other users in the cluster. This issue is fixed in Elasticsearch 7.10.2 CVE ID : CVE-2021-22132	https://discuss.elastic.co/t/elasticsearch-7-10-2-security-update/261164	A-ELA-ELAS-210121/81
evolucare					
ecs_imaging					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jan-21	10	** UNSUPPORTED WHEN ASSIGNED ** EVOLUCARE ECSIMAGING (aka ECS Imaging) through 6.21.5 has an OS Command Injection vulnerability via shell metacharacters and an IFS manipulation. The parameter "file" on the webpage /showfile.php can be exploited to gain root access. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. CVE ID : CVE-2021-3029	N/A	A-EVO-ECS_-210121/82

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
flask-security-too_project										
flask-security-too										
Cross-Site Request Forgery (CSRF)	11-Jan-21	4.3	<p>The Python "Flask-Security-Too" package is used for adding security features to your Flask application. It is an independently maintained version of Flask-Security based on the 3.0.0 version of Flask-Security. In Flask-Security-Too from version 3.3.0 and before version 3.4.5, the /login and /change endpoints can return the authenticated user's authentication token in response to a GET request. Since GET requests aren't protected with a CSRF token, this could lead to a malicious 3rd party site acquiring the authentication token. Version 3.4.5 and version 4.0.0 are patched. As a workaround, if you aren't using authentication tokens - you can set the SECURITY_TOKEN_MAX_AGE to "0" (seconds) which should make the token unusable.</p> <p>CVE ID : CVE-2021-21241</p>	<p>https://github.com/Flask-Middleware/flask-security/commit/61d313150b5f620d0b800896c4f2199005e84b1f, https://github.com/Flask-Middleware/flask-security/commit/6d50ee9169acf813257c37b75babe9c28e83542a</p>	A-FLA-FLAS-210121/83					
getlaminas										
laminas-http										
Deserialization of Untrusted Data	04-Jan-21	7.5	<p>** DISPUTED ** Laminas Project laminas-http before 2.14.2, and Zend Framework 3.0.0, has a deserialization vulnerability that can lead to</p>	<p>https://github.com/laminas/laminas-http/commit</p>	A-GET-LAMI-210121/84					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote code execution if the content is controllable, related to the __destruct method of the Zend\Http\Response\Stream class in Stream.php. NOTE: Zend Framework is no longer supported by the maintainer. NOTE: the laminas-http vendor considers this a "vulnerability in the PHP language itself" but has added certain type checking as a way to prevent exploitation in (unrecommended) use cases where attacker-supplied data can be deserialized. CVE ID : CVE-2021-3007	s/2.15.x/src/Response/Stream.php, https://github.com/laminas/laminas-http/pull/48	
git-big-picture_project					
git-big-picture					
Improper Input Validation	13-Jan-21	7.5	git-big-picture before 1.0.0 mishandles ' characters in a branch name, leading to code execution. CVE ID : CVE-2021-3028	https://github.com/git-big-picture/git-big-picture/pull/27 , https://github.com/git-big-picture/git-big-picture/pull/62	A-GIT-GIT--210121/85
Golang					
protobuf					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	11-Jan-21	7.5	An issue was discovered in GoGo Protobuf before 1.3.2. plugin/unmarshal/unmarshal.go lacks certain index validation, aka the "skippy peanut butter" issue. CVE ID : CVE-2021-3121	https://github.com/gogo/protobuf/commit/b03c65ea87cdc3521ede29f62fe3ce239267c1bc , https://github.com/gogo/protobuf/compare/v1.3.1...v1.3.2	A-GOL-PROT-210121/86
Google					
chrome					
Use After Free	08-Jan-21	6.8	Use after free in payments in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21109	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html , https://crbug.com/1152334	A-GOO-CHRO-210121/87
Use After Free	08-Jan-21	6.8	Use after free in safe browsing in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21110	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html , https://crbug.com/1152451	A-GOO-CHRO-210121/88

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Rendered UI Layers or Frames	08-Jan-21	6.8	Insufficient policy enforcement in WebUI in Google Chrome prior to 87.0.4280.141 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. CVE ID : CVE-2021-21111	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html , https://crbug.com/1149125	A-GOO-CHRO-210121/89
Use After Free	08-Jan-21	6.8	Use after free in Blink in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21112	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html , https://crbug.com/1151298	A-GOO-CHRO-210121/90
Out-of-bounds Write	08-Jan-21	6.8	Heap buffer overflow in Skia in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21113	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html , https://crbug.com/1155178	A-GOO-CHRO-210121/91
Use After Free	08-Jan-21	6.8	Use after free in audio in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to	https://chromereleases.googleblog.com/2021/01/	A-GOO-CHRO-210121/92

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21114	stable-channel-update-for-desktop.html , https://crbug.com/1150065	
Use After Free	08-Jan-21	6.8	User after free in safe browsing in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21115	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html , https://crbug.com/1157814	A-GOO-CHRO-210121/93
Out-of-bounds Write	08-Jan-21	6.8	Heap buffer overflow in audio in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21116	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html , https://crbug.com/1151069	A-GOO-CHRO-210121/94
Use After Free	08-Jan-21	9.3	Use after free in autofill in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html	A-GOO-CHRO-210121/95

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21106	, https://crbug.com/1148749	
Use After Free	08-Jan-21	6.8	Use after free in drag and drop in Google Chrome on Linux prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21107	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html , https://crbug.com/1153595	A-GOO-CHRO-210121/96
Use After Free	08-Jan-21	6.8	Use after free in media in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21108	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html , https://crbug.com/1155426	A-GOO-CHRO-210121/97

invisioncommunity

ips_community_suite

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jan-21	6.5	Invision Community IPS Community Suite before 4.5.4.2 allows SQL Injection via the Downloads REST API (the sortDir parameter in a sortBy=popular action to the GETindex() method in applications/downloads/api/files.php).	https://invisioncommunity.com/release-notes/	A-INV-IPS_-210121/98
--	-----------	-----	--	---	----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-3025		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-21	4.3	Invision Community IPS Community Suite before 4.5.4.2 allows XSS during the quoting of a post or comment. CVE ID : CVE-2021-3026	https://invisioncommunity.com/release-notes/	A-INV-IPS-210121/99
ipeak					
ipeakcms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jan-21	7.5	ipeak Infosystems ibexwebCMS (aka IPeakCMS) 3.5 is vulnerable to an unauthenticated Boolean-based SQL injection via the id parameter on the /cms/print.php page. CVE ID : CVE-2021-3018	https://ipeak.ch	A-IPE-IPEA-210121/100
ispconfig					
ispconfig					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jan-21	7.5	ISPConfig before 3.2.2 allows SQL injection. CVE ID : CVE-2021-3021	https://www.ispconfig.org/blog/ispconfig-3-2-2-released-important-security-update/	A-ISP-ISPC-210121/101
Jenkins					
bumblebee_hp_alm					
Insufficiently Protected Credentials	13-Jan-21	2.1	Jenkins Bumblebee HP ALM Plugin 4.1.5 and earlier stores credentials unencrypted in its global configuration file on the	https://www.jenkins.io/security/advisory/2021-01-	A-JEN-BUMB-210121/102

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Jenkins controller where they can be viewed by users with access to the Jenkins controller file system. CVE ID : CVE-2021-21614	13/#SECURITY-2156						
tracetronic_ecu-test										
Insufficiently Protected Credentials	13-Jan-21	2.1	Jenkins TraceTronic ECU-TEST Plugin 2.23.1 and earlier stores credentials unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system. CVE ID : CVE-2021-21612	https://www.jenkins.io/security/advisory/2021-01-13/#SECURITY-2057	A-JEN-TRAC-210121/103					
tics										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	4.3	Jenkins TICS Plugin 2020.3.0.6 and earlier does not escape TICS service responses, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers able to control TICS service response content. CVE ID : CVE-2021-21613	https://www.jenkins.io/security/advisory/2021-01-13/#SECURITY-2098	A-JEN-TICS-210121/104					
jenkins										
Improper Link Resolution Before File Access ('Link Following')	13-Jan-21	4	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows reading arbitrary files using the file browser for workspaces and archived artifacts by following symlinks. CVE ID : CVE-2021-21602	https://www.jenkins.io/security/advisory/2021-01-13/#SECURITY-1452	A-JEN-JENK-210121/105					
Improper Neutralization	13-Jan-21	3.5	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does	https://www.jenkins.io/	A-JEN-JENK-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			not escape notification bar response contents, resulting in a cross-site scripting (XSS) vulnerability. CVE ID : CVE-2021-21603	security/adv isory/2021-01-13/#SECURITY-1889	210121/106
Deserializati on of Untrusted Data	13-Jan-21	6	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows attackers with permission to create or configure various objects to inject crafted content into Old Data Monitor that results in the instantiation of potentially unsafe objects once discarded by an administrator. CVE ID : CVE-2021-21604	https://www.jenkins.io/security/adv isory/2021-01-13/#SECURITY-1923	A-JEN-JENK-210121/107
Improper Input Validation	13-Jan-21	6	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows users with Agent/Configure permission to choose agent names that cause Jenkins to override the global `config.xml` file. CVE ID : CVE-2021-21605	https://www.jenkins.io/security/adv isory/2021-01-13/#SECURITY-2021	A-JEN-JENK-210121/108
Improper Input Validation	13-Jan-21	4	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier improperly validates the format of a provided fingerprint ID when checking for its existence allowing an attacker to check for the existence of XML files with a short path. CVE ID : CVE-2021-21606	https://www.jenkins.io/security/adv isory/2021-01-13/#SECURITY-2023	A-JEN-JENK-210121/109
Allocation of Resources Without	13-Jan-21	4	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not limit sizes provided as	https://www.jenkins.io/security/adv isory/2021-01-13/#SECURITY-2023	A-JEN-JENK-210121/110

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			query parameters to graph-rendering URLs, allowing attackers to request crafted URLs that use all available memory in Jenkins, potentially leading to out of memory errors. CVE ID : CVE-2021-21607	isory/2021-01-13/#SECURITY-2025	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not escape button labels in the Jenkins UI, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers with the ability to control button labels. CVE ID : CVE-2021-21608	https://www.jenkins.io/security/advisory/2021-01-13/#SECURITY-2035	A-JEN-JENK-210121/111
Incorrect Authorization	13-Jan-21	5	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not correctly match requested URLs to the list of always accessible paths, allowing attackers without Overall/Read permission to access some URLs as if they did have Overall/Read permission. CVE ID : CVE-2021-21609	https://www.jenkins.io/security/advisory/2021-01-13/#SECURITY-2047	A-JEN-JENK-210121/112
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	4.3	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not implement any restrictions for the URL rendering a formatted preview of markup passed as a query parameter, resulting in a reflected cross-site scripting (XSS) vulnerability if the configured markup formatter does not prohibit	https://www.jenkins.io/security/advisory/2021-01-13/#SECURITY-2153	A-JEN-JENK-210121/113

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unsafe elements (JavaScript) in markup. CVE ID : CVE-2021-21610		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not escape display names and IDs of item types shown on the New Item page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to specify display names or IDs of item types. CVE ID : CVE-2021-21611	https://www.jenkins.io/security/advisory/2021-01-13/#SECURITY-2171	A-JEN-JENK-210121/114
Joomla					
joomla\!					
Missing Authorization	12-Jan-21	5	An issue was discovered in Joomla! 3.0.0 through 3.9.23. The lack of ACL checks in the orderPosition endpoint of com_modules leak names of unpublished and/or inaccessible modules. CVE ID : CVE-2021-23123	https://developer.joomla.org/security-centre/836-20210101-core-com-modules-exposes-module-names.html	A-JOO-JOOM-210121/115
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jan-21	4.3	An issue was discovered in Joomla! 3.9.0 through 3.9.23. The lack of escaping in mod_breadcrumbs aria-label attribute allows XSS attacks. CVE ID : CVE-2021-23124	https://developer.joomla.org/security-centre/837-20210102-core-xss-in-mod-breadcrumbs-aria-label-attribute.html	A-JOO-JOOM-210121/116

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jan-21	4.3	An issue was discovered in Joomla! 3.1.0 through 3.9.23. The lack of escaping of image-related parameters in multiple com_tags views cause lead to XSS attack vectors. CVE ID : CVE-2021-23125	https://developer.joomla.org/security-centre/838-20210103-core-xss-in-com-tags-image-parameters.html	A-JOO-JOOM-210121/117

jqueryvalidation

jquery_validation

Uncontrolled Resource Consumption	13-Jan-21	5	The jQuery Validation Plugin provides drop-in validation for your existing forms. It is published as an npm package "jquery-validation". jquery-validation before version 1.19.3 contains one or more regular expressions that are vulnerable to ReDoS (Regular Expression Denial of Service). This is fixed in 1.19.3. CVE ID : CVE-2021-21252	https://github.com/jquery-validation/jquery-validation/commit/5d8f29eef363d043a8fec4eb86d42cadb5fa5f7d , https://github.com/jquery-validation/jquery-validation/pull/2371	A-JQU-JQUE-210121/118
-----------------------------------	-----------	---	---	--	-----------------------

kamadak-exif_project

kamadak-exif

Uncontrolled Resource Consumption	06-Jan-21	4.3	kamadak-exif is an exif parsing library written in pure Rust. In kamadak-exif version 0.5.2, there is an infinite loop in parsing crafted PNG files. Specifically,	https://github.com/kamadak/exif-rs/commit/f21df24616ea611c5d5d0e0e2f8042e	A-KAM-KAMA-210121/119
-----------------------------------	-----------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reader::read_from_container can cause an infinite loop when a crafted PNG file is given. This is fixed in version 0.5.3. No workaround is available. Applications that do not pass files with the PNG signature to Reader::read_from_container are not affected. CVE ID : CVE-2021-21235	b74d5ff48, https://github.com/kamadadak/exif-rs/security/advisories/GHSA-px9g-8hgv-jvg2	

lanproxy_project

lanproxy

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jan-21	5	ffay lanproxy 0.1 allows Directory Traversal to read ../conf/config.properties to obtain credentials for a connection to the intranet. CVE ID : CVE-2021-3019	https://github.com/ffay/lanproxy/commits/master	A-LAN-LANP-210121/120
--	-----------	---	---	---	-----------------------

medicalexp

ecs_imaging

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Jan-21	7.5	** UNSUPPORTED WHEN ASSIGNED ** EVOLUCARE ECSIMAGING (aka ECS Imaging) through 6.21.5 has multiple SQL Injection issues in the login form and the password-forgotten form (such as /req_password_user.php?email=). This allows an attacker to steal data in the database and obtain access to the application. (The database component runs as root.) NOTE: This vulnerability only affects products that	N/A	A-MED-ECS_-210121/121
--	-----------	-----	---	-----	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are no longer supported by the maintainer. CVE ID : CVE-2021-3118		
Microsoft					
365_apps					
Not Available	12-Jan-21	9.3	Microsoft Office Remote Code Execution Vulnerability CVE ID : CVE-2021-1711	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1711	A-MIC-365_-210121/122
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jan-21	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1714. CVE ID : CVE-2021-1713	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1713	A-MIC-365_-210121/123
Not Available	12-Jan-21	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1713. CVE ID : CVE-2021-1714	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1714	A-MIC-365_-210121/124
Out-of-bounds Write	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1716. CVE ID : CVE-2021-1715	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1715	A-MIC-365_-210121/125
Not Available	12-Jan-21	9.3	Microsoft Word Remote	https://portal	A-MIC-365_-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability This CVE ID is unique from CVE-2021-1715. CVE ID : CVE-2021-1716	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1716	210121/126
office_web_apps					
Out-of-bounds Write	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1716. CVE ID : CVE-2021-1715	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1715	A-MIC-OFFI-210121/127
Not Available	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1715. CVE ID : CVE-2021-1716	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1716	A-MIC-OFFI-210121/128
windows_defender					
Not Available	12-Jan-21	7.2	Microsoft Defender Remote Code Execution Vulnerability CVE ID : CVE-2021-1647	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1647	A-MIC-WIND-210121/129
system_center_endpoint_protection					
Not Available	12-Jan-21	7.2	Microsoft Defender Remote Code Execution Vulnerability CVE ID : CVE-2021-1647	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-SYST-210121/130

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2021-1647	
bot_framework_software_development_kit					
Exposure of Sensitive Information to an Unauthorized Actor	12-Jan-21	2.1	Bot Framework SDK Information Disclosure Vulnerability CVE ID : CVE-2021-1725	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1725	A-MIC-BOT_-210121/131
hevc_video_extensions					
Not Available	12-Jan-21	9.3	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1644. CVE ID : CVE-2021-1643	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1643	A-MIC-HEVC-210121/132
Not Available	12-Jan-21	9.3	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1643. CVE ID : CVE-2021-1644	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1644	A-MIC-HEVC-210121/133
security_essentials					
Not Available	12-Jan-21	7.2	Microsoft Defender Remote Code Execution Vulnerability CVE ID : CVE-2021-1647	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1647	A-MIC-SECU-210121/134

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
visual_studio					
Improper Privilege Management	12-Jan-21	7.2	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1680. CVE ID : CVE-2021-1651	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1651	A-MIC-VISU-210121/135
office					
Not Available	12-Jan-21	9.3	Microsoft Office Remote Code Execution Vulnerability CVE ID : CVE-2021-1711	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1711	A-MIC-OFFI-210121/136
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jan-21	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1714. CVE ID : CVE-2021-1713	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1713	A-MIC-OFFI-210121/137
Not Available	12-Jan-21	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1713. CVE ID : CVE-2021-1714	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1714	A-MIC-OFFI-210121/138
Out-of-bounds Write	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1716.	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-OFFI-210121/139

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1715	guidance/advisory/CVE-2021-1715	
Not Available	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1715. CVE ID : CVE-2021-1716	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1716	A-MIC-OFFI-210121/140
visual_studio_2017					
Improper Privilege Management	12-Jan-21	7.2	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1680. CVE ID : CVE-2021-1651	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1651	A-MIC-VISU-210121/141
asp.net_core					
Not Available	12-Jan-21	5	ASP.NET Core and Visual Studio Denial of Service Vulnerability CVE ID : CVE-2021-1723	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1723	A-MIC-ASP.-210121/142
sharepoint_server					
Improper Input Validation	12-Jan-21	5.8	Microsoft SharePoint Spoofing Vulnerability This CVE ID is unique from CVE-2021-1717. CVE ID : CVE-2021-1641	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1641	A-MIC-SHAR-210121/143

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	12-Jan-21	9	Microsoft SharePoint Server Remote Code Execution Vulnerability CVE ID : CVE-2021-1707	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1707	A-MIC-SHAR-210121/144
Improper Privilege Management	12-Jan-21	6	Microsoft SharePoint Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1719. CVE ID : CVE-2021-1712	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1712	A-MIC-SHAR-210121/145
Out-of-bounds Write	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1716. CVE ID : CVE-2021-1715	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1715	A-MIC-SHAR-210121/146
Not Available	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1715. CVE ID : CVE-2021-1716	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1716	A-MIC-SHAR-210121/147
Improper Input Validation	12-Jan-21	5.8	Microsoft SharePoint Spoofing Vulnerability This CVE ID is unique from CVE-2021-1641. CVE ID : CVE-2021-1717	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1717	A-MIC-SHAR-210121/148

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-1717	
Improper Privilege Management	12-Jan-21	6	Microsoft SharePoint Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1712. CVE ID : CVE-2021-1719	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1719	A-MIC-SHAR-210121/149
office_web_apps_server					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jan-21	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1714. CVE ID : CVE-2021-1713	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1713	A-MIC-OFFI-210121/150
Not Available	12-Jan-21	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1713. CVE ID : CVE-2021-1714	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1714	A-MIC-OFFI-210121/151
Out-of-bounds Write	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1716. CVE ID : CVE-2021-1715	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1715	A-MIC-OFFI-210121/152
Not Available	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1715.	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-OFFI-210121/153

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2021-1716	guidance/advisory/CVE-2021-1716						
word										
Out-of-bounds Write	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1716. CVE ID : CVE-2021-1715	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1715	A-MIC-WORD-210121/154					
Not Available	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1715. CVE ID : CVE-2021-1716	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1716	A-MIC-WORD-210121/155					
sharepoint_enterprise_server										
Improper Input Validation	12-Jan-21	5.8	Microsoft SharePoint Spoofing Vulnerability This CVE ID is unique from CVE-2021-1717. CVE ID : CVE-2021-1641	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1641	A-MIC-SHAR-210121/156					
Not Available	12-Jan-21	9	Microsoft SharePoint Server Remote Code Execution Vulnerability CVE ID : CVE-2021-1707	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1707	A-MIC-SHAR-210121/157					
Improper Privilege	12-Jan-21	6	Microsoft SharePoint Elevation of Privilege	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1707	A-MIC-SHAR-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Vulnerability This CVE ID is unique from CVE-2021-1719. CVE ID : CVE-2021-1712	osoft.com/en-US/security-guidance/advisory/CVE-2021-1712	210121/158
Not Available	12-Jan-21	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1713. CVE ID : CVE-2021-1714	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1714	A-MIC-SHAR-210121/159
Out-of-bounds Write	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1716. CVE ID : CVE-2021-1715	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1715	A-MIC-SHAR-210121/160
Not Available	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1715. CVE ID : CVE-2021-1716	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1716	A-MIC-SHAR-210121/161
Improper Input Validation	12-Jan-21	5.8	Microsoft SharePoint Spoofing Vulnerability This CVE ID is unique from CVE-2021-1641. CVE ID : CVE-2021-1717	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1717	A-MIC-SHAR-210121/162
Improper	12-Jan-21	6	Microsoft SharePoint	https://port	A-MIC-SHAR-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1712. CVE ID : CVE-2021-1719	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1719	210121/163
office_online_server					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jan-21	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1714. CVE ID : CVE-2021-1713	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1713	A-MIC-OFFI-210121/164
Not Available	12-Jan-21	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1713. CVE ID : CVE-2021-1714	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1714	A-MIC-OFFI-210121/165
Out-of-bounds Write	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1716. CVE ID : CVE-2021-1715	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1715	A-MIC-OFFI-210121/166
Not Available	12-Jan-21	9.3	Microsoft Word Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1715. CVE ID : CVE-2021-1716	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1716	A-MIC-OFFI-210121/167

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-1716	
sharepoint_foundation					
Improper Input Validation	12-Jan-21	5.8	Microsoft SharePoint Spoofing Vulnerability This CVE ID is unique from CVE-2021-1717. CVE ID : CVE-2021-1641	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1641	A-MIC-SHAR-210121/168
Not Available	12-Jan-21	9	Microsoft SharePoint Server Remote Code Execution Vulnerability CVE ID : CVE-2021-1707	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1707	A-MIC-SHAR-210121/169
Improper Privilege Management	12-Jan-21	6	Microsoft SharePoint Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1719. CVE ID : CVE-2021-1712	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1712	A-MIC-SHAR-210121/170
Improper Input Validation	12-Jan-21	5.8	Microsoft SharePoint Spoofing Vulnerability This CVE ID is unique from CVE-2021-1641. CVE ID : CVE-2021-1717	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1717	A-MIC-SHAR-210121/171
Not Available	12-Jan-21	6.5	Microsoft SharePoint Server Tampering Vulnerability CVE ID : CVE-2021-1718	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-SHAR-210121/172

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2021-1718	
excel					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jan-21	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1714. CVE ID : CVE-2021-1713	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1713	A-MIC-EXCE-210121/173
Not Available	12-Jan-21	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1713. CVE ID : CVE-2021-1714	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1714	A-MIC-EXCE-210121/174
excel_services					
Not Available	12-Jan-21	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1713. CVE ID : CVE-2021-1714	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1714	A-MIC-EXCE-210121/175
visual_studio_2019					
Not Available	12-Jan-21	5	ASP.NET Core and Visual Studio Denial of Service Vulnerability CVE ID : CVE-2021-1723	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1723	A-MIC-VISU-210121/176

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jan-21	7.2	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1680. CVE ID : CVE-2021-1651	https://portal.msrf.com/en-US/security-guidance/advisory/CVE-2021-1651	A-MIC-VISU-210121/177
sql_server					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Jan-21	6.5	Microsoft SQL Elevation of Privilege Vulnerability CVE ID : CVE-2021-1636	https://portal.msrf.com/en-US/security-guidance/advisory/CVE-2021-1636	A-MIC-SQL_-210121/178
mk-auth					
mk-auth					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-21	3.5	MK-AUTH through 19.01 K4.9 allows XSS via the admin/logs_ajax.php tipo parameter. An attacker can leverage this to read the centralmka2 (session token) cookie, which is not set to HTTPOnly. CVE ID : CVE-2021-21494	http://mk-auth.com.br/	A-MK--MK-A-210121/179
Cross-Site Request Forgery (CSRF)	04-Jan-21	6.8	MK-AUTH through 19.01 K4.9 allows CSRF for password changes via the central/executar_central.php?acao=altsenha_princ URI. CVE ID : CVE-2021-21495	http://mk-auth.com.br/	A-MK--MK-A-210121/180
Not Available	03-Jan-21	4	MK-AUTH through 19.01 K4.9 allows remote attackers to obtain sensitive	http://mk-auth.com.br/	A-MK--MK-A-210121/181

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			information (e.g., a CPF number) via a modified titulo (aka invoice number) value to the central/recibo.php URI. CVE ID : CVE-2021-3005							
mubu										
mubu										
Improper Privilege Management	12-Jan-21	4.6	Mubu 2.2.1 allows local users to gain privileges to execute commands, aka CNVD-2020-68878. CVE ID : CVE-2021-3134	http://mubu.com/doc/d5501245199	A-MUB-MUBU-210121/182					
Nvidia										
gpu_driver										
Improper Privilege Management	08-Jan-21	7.2	NVIDIA GPU Display Driver for Windows, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which an operation is performed which may lead to denial of service or escalation of privileges. CVE ID : CVE-2021-1051	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-GPU_-210121/183					
Improper Privilege Management	08-Jan-21	7.2	NVIDIA GPU Display Driver for Windows and Linux, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape or IOCTL in which user-mode clients can access legacy privileged APIs, which may lead to denial of service, escalation of privileges, and information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-GPU_-210121/184					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1052		
Improper Input Validation	08-Jan-21	2.1	NVIDIA GPU Display Driver for Windows and Linux, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape or IOCTL in which improper validation of a user pointer may lead to denial of service. CVE ID : CVE-2021-1053	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-GPU_-210121/185
Incorrect Authorization	08-Jan-21	2.1	NVIDIA GPU Display Driver for Windows, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which the software does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action, which may lead to denial of service. CVE ID : CVE-2021-1054	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-GPU_-210121/186
Incorrect Authorization	08-Jan-21	4.6	NVIDIA GPU Display Driver for Windows, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which improper access control may lead to denial of service and information disclosure. CVE ID : CVE-2021-1055	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-GPU_-210121/187
Incorrect Default Permissions	08-Jan-21	3.6	NVIDIA GPU Display Driver for Linux, all versions, contains a vulnerability in the kernel mode layer	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-GPU_-210121/188

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(nvidia.ko) in which it does not completely honor operating system file system permissions to provide GPU device-level isolation, which may lead to denial of service or information disclosure. CVE ID : CVE-2021-1056	a_id/5142	
virtual_gpu_manager					
Allocation of Resources Without Limits or Throttling	08-Jan-21	4.6	NVIDIA Virtual GPU Manager NVIDIA vGPU manager contains a vulnerability in the vGPU plugin in which it allows guests to allocate some resources for which the guest is not authorized, which may lead to integrity and confidentiality loss, denial of service, or information disclosure. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1057	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-VIRT-210121/189
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input data size is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1058	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-VIRT-210121/190
Integer Overflow or Wraparound	08-Jan-21	4.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input index is not validated,	https://nvidia.custhelp.com/app/answers/detail/	A-NVI-VIRT-210121/191

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which may lead to integer overflow, which in turn may cause tampering of data, information disclosure, or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1059	a_id/5142	
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input index is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1060	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-VIRT-210121/192
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-21	3.3	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which a race condition may cause the vGPU plugin to continue using a previously validated resource that has since changed, which may lead to denial of service or information disclosure. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1061	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-VIRT-210121/193
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input data length is not validated, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-VIRT-210121/194

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1062		
Out-of-bounds Read	08-Jan-21	4.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input offset is not validated, which may lead to a buffer overread, which in turn may cause tampering of data, information disclosure, or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1063	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-VIRT-210121/195
NULL Pointer Dereference	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which it obtains a value from an untrusted source, converts this value to a pointer, and dereferences the resulting pointer, which may lead to information disclosure or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1064	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-VIRT-210121/196
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which input data is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-VIRT-210121/197

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1065		
Uncontrolled Resource Consumption	08-Jan-21	2.1	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which input data is not validated, which may lead to unexpected consumption of resources, which in turn may lead to denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1066	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	A-NVI-VIRT-210121/198

Open-xchange

open-xchange_appsuite

Server-Side Request Forgery (SSRF)	12-Jan-21	5.5	OX App Suite through 7.10.4 allows SSRF via a URL with an @ character in an appsuite/api/oauth/proxy PUT request. CVE ID : CVE-2021-23927	N/A	A-OPE-OPEN-210121/199
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jan-21	4.3	OX App Suite through 7.10.3 allows XSS via the ajax/apps/manifests query string. CVE ID : CVE-2021-23928	N/A	A-OPE-OPEN-210121/200
Improper Neutralization of Input During Web Page Generation ('Cross-site	12-Jan-21	4.3	OX App Suite through 7.10.4 allows XSS via a crafted Content-Disposition header in an uploaded HTML document to an ajax/share/<share-token>?delivery=view URI.	N/A	A-OPE-OPEN-210121/201

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			CVE ID : CVE-2021-23929		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jan-21	4.3	OX App Suite through 7.10.4 allows XSS via use of the conversion API for a distributedFile. CVE ID : CVE-2021-23930	N/A	A-OPE-OPEN-210121/202
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jan-21	4.3	OX App Suite through 7.10.4 allows XSS via an inline binary file. CVE ID : CVE-2021-23931	N/A	A-OPE-OPEN-210121/203
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jan-21	4.3	OX App Suite through 7.10.4 allows XSS via an inline image with a crafted filename. CVE ID : CVE-2021-23932	N/A	A-OPE-OPEN-210121/204
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jan-21	4.3	OX App Suite through 7.10.4 allows XSS via JavaScript in a Note referenced by a mail:// URL. CVE ID : CVE-2021-23933	N/A	A-OPE-OPEN-210121/205
Improper Neutralization of Input During Web Page Generation	12-Jan-21	4.3	OX App Suite through 7.10.4 allows XSS via a contact whose name contains JavaScript code. CVE ID : CVE-2021-23934	N/A	A-OPE-OPEN-210121/206

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jan-21	4.3	OX App Suite through 7.10.4 allows XSS via an appointment in which the location contains JavaScript code. CVE ID : CVE-2021-23935	N/A	A-OPE-OPEN-210121/207
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jan-21	4.3	OX App Suite through 7.10.4 allows XSS via the subject of a task. CVE ID : CVE-2021-23936	N/A	A-OPE-OPEN-210121/208
Opera					
opera_mini					
Not Available	11-Jan-21	5	Opera Mini for Android below 53.1 displays URL left-aligned in the address field. This allows a malicious attacker to craft a URL with a long domain name, e.g. www.safe.opera.com.attacker.com. With the URL being left-aligned, the user will only see the front part (e.g. www.safe.opera.com...) The exact amount depends on the phone screen size but the attacker can craft a number of different domains and target different phones. Starting with version 53.1 Opera Mini displays long URLs with the top-level	https://security.opera.com/address-bar-spoofing-in-opera-mini-opera-security-advisories/	A-OPE-OPER-210121/209

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			domain label aligned to the right of the address field which mitigates the issue. CVE ID : CVE-2021-23253		
Owasp					
json-sanitizer					
Improper Restriction of XML External Entity Reference	13-Jan-21	7.5	OWASP json-sanitizer before 1.2.2 may emit closing SCRIPT tags and CDATA section delimiters for crafted input. This allows an attacker to inject arbitrary HTML or XML into embedding documents. CVE ID : CVE-2021-23899	https://github.com/OWASP/json-sanitizer/commit/a37f594f7378a1c76b3283e0dab9e1ab1dc0247e , https://github.com/OWASP/json-sanitizer/compare/v1.2.1...v1.2.2	A-OWA-JSON-210121/210
Not Available	13-Jan-21	5	OWASP json-sanitizer before 1.2.2 can output invalid JSON or throw an undeclared exception for crafted input. This may lead to denial of service if the application is not prepared to handle these situations. CVE ID : CVE-2021-23900	https://github.com/OWASP/json-sanitizer/commit/a37f594f7378a1c76b3283e0dab9e1ab1dc0247e , https://github.com/OWASP/json-sanitizer/compare/v1.2.1...v1.2.2	A-OWA-JSON-210121/211
proxy.py_project					
proxy.py					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	11-Jan-21	5	before_upstream_connection in AuthPlugin in http/proxy/auth.py in proxy.py before 2.3.1 accepts incorrect Proxy-Authorization header data because of a boolean confusion (and versus or). CVE ID : CVE-2021-3116	https://github.com/abhinavsinh/proxy.py/pull/482/commit/s/9b00093288237f5073c403f2c4f62acfdfa8ed46	A-PRO-PROX-210121/212
SAP					
graphical_user_interface					
Insufficiently Protected Credentials	12-Jan-21	2.1	SAP GUI for Windows, version - 7.60, allows an attacker to spoof logon credentials for Application Server ABAP backend systems in the client PCs memory. Under certain conditions the attacker can access information which would otherwise be restricted. The exploit can only be executed locally on the client PC and not via Network and the attacker needs at least user authorization of the Operating System user of the victim. CVE ID : CVE-2021-21448	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-GRAP-210121/213
netweaver_master_data_management					
Exposure of Sensitive Information to an Unauthorized Actor	12-Jan-21	5	When security guidelines for SAP NetWeaver Master Data Management, versions 7.10, 710, and 710.750, running on windows have not been thoroughly reviewed, it might be possible for an external operator to try and	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-NETW-210121/214

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>set custom paths in the MDS server configuration. When no adequate protection has been enforced on any level (e.g., MDS Server password not set, network and OS configuration not properly secured, etc.), a malicious user might define UNC paths which could then be exploited to put the system at risk using a so-called SMB relay attack and obtain highly sensitive data, which leads to Information Disclosure.</p> <p>CVE ID : CVE-2021-21469</p>		

3d_visual_enterprise_viewer

Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jan-21	6.8	<p>SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated IFF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.</p> <p>CVE ID : CVE-2021-21449</p>	<p>https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476</p>	A-SAP-3D_V-210121/215
---	-----------	-----	---	--	-----------------------

Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jan-21	6.8	<p>SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PSD file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable</p>	<p>https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476</p>	A-SAP-3D_V-210121/216
---	-----------	-----	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21450		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated SGI file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21451	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/217
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated GIF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21452	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/218
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated RLE file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/219

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21453		
Out-of-bounds Write	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated RLE file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21454	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/220
Out-of-bounds Write	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated DIB file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21455	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/221
Out-of-bounds Write	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated DIB file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/222

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21456		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated IFF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21457	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/223
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated IFF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21458	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/224
Out-of-bounds Write	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated IFF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/225

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21459		
Out-of-bounds Write	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated DIB file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21460	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/226
Out-of-bounds Write	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated BMP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21461	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/227
Out-of-bounds Write	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/228

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21462		
Out-of-bounds Read	12-Jan-21	6.8	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21463	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/229
Not Available	12-Jan-21	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. CVE ID : CVE-2021-21464	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-3D_V-210121/230
enterprise_performance_management					
Improper Restriction of XML External Entity Reference	12-Jan-21	3.6	SAP EPM Add-in for Microsoft Office, version - 1010 and SAP EPM Add-in for SAP Analysis Office, version - 2.8, allows an authenticated attacker with user privileges to parse	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-ENTE-210121/231

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious XML files which could result in XXE-based attacks in applications that accept attacker-controlled XML configuration files. This occurs as logging service does not disable XML external entities when parsing configuration files and a successful exploit would result in limited impact on integrity and availability of the application. CVE ID : CVE-2021-21470		
cla-assistant					
Not Available	12-Jan-21	4	In CLA-Assistant, versions before 2.8.5, due to improper access control an authenticated user could access API endpoints which are not intended to be used by the user. This could impact the integrity of the application. CVE ID : CVE-2021-21471	https://github.com/cla-assistant/cla-assistant/security/advisories/GHSA-4h6f-c68c-pxhr	A-SAP-CLA--210121/232
business_warehouse					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Jan-21	6.5	The BW Database Interface allows an attacker with low privileges to execute any crafted database queries, exposing the backend database. An attacker can include their own SQL commands which the database will execute without properly sanitizing the untrusted data leading to SQL injection vulnerability	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-BUSI-210121/233

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which can fully compromise the affected SAP system. CVE ID : CVE-2021-21465		
Improper Control of Generation of Code ('Code Injection')	12-Jan-21	6.5	SAP Business Warehouse, versions 700, 701, 702, 711, 730, 731, 740, 750, 782 and SAP BW/4HANA, versions 100, 200, allow a low privileged attacker to inject code using a remote enabled function module over the network. Via the function module an attacker can create a malicious ABAP report which could be used to get access to sensitive data, to inject malicious UPDATE statements that could have also impact on the operating system, to disrupt the functionality of the SAP system which can thereby lead to a Denial of Service. CVE ID : CVE-2021-21466	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-BUSI-210121/234
Missing Authorization	12-Jan-21	4	The BW Database Interface does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges that allows the user to practically read out any database table. CVE ID : CVE-2021-21468	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-BUSI-210121/235
banking_services					
Missing Authorization	12-Jan-21	4	SAP Banking Services (Generic Market Data) 400, 450, and 500 does not perform necessary	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-BANK-210121/236

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization checks for an authenticated user, resulting in escalation of privileges. An unauthorized User is allowed to display restricted Business Partner Generic Market Data (GMD), due to improper authorization check. CVE ID : CVE-2021-21467	ion?pagelId=564760476	
businessobjects_business_intelligence					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jan-21	3.5	SAP BusinessObjects Business Intelligence platform, versions 410, 420, allows an authenticated attacker to inject malicious JavaScript payload into the custom value input field of an Input Control, which can be executed by User who views the relevant application content, which leads to Stored Cross-Site Scripting. CVE ID : CVE-2021-21447	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pagelId=564760476	A-SAP-BUSI-210121/237
bw\4hana					
Improper Control of Generation of Code ('Code Injection')	12-Jan-21	6.5	SAP Business Warehouse, versions 700, 701, 702, 711, 730, 731, 740, 750, 782 and SAP BW/4HANA, versions 100, 200, allow a low privileged attacker to inject code using a remote enabled function module over the network. Via the function module an attacker can create a malicious ABAP report which could be used to get access to sensitive	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pagelId=564760476	A-SAP-BW\/-210121/238

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data, to inject malicious UPDATE statements that could have also impact on the operating system, to disrupt the functionality of the SAP system which can thereby lead to a Denial of Service. CVE ID : CVE-2021-21466		
netweaver_as_abap					
Uncontrolled Resource Consumption	12-Jan-21	5	SAP NetWeaver AS ABAP, versions 740, 750, 751, 752, 753, 754, 755, allows an unauthenticated attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service, this has a high impact on the availability of the service. CVE ID : CVE-2021-21446	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-NETW-210121/239
commerce_cloud					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	12-Jan-21	3.5	SAP Commerce Cloud, versions - 1808, 1811, 1905, 2005, 2011, allows an authenticated attacker to include invalidated data in the HTTP response Content Type header, due to improper input validation, and sent to a Web user. A successful exploitation of this vulnerability may lead to advanced attacks, including cross-site scripting and page hijacking. CVE ID : CVE-2021-21445	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476	A-SAP-COMM-210121/240
seal_finance_project					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
seal_finance					
Incorrect Authorization	03-Jan-21	5	The breed function in the smart contract implementation for Farm in Seal Finance (Seal), an Ethereum token, lacks access control and thus allows price manipulation, as exploited in the wild in December 2020 and January 2021. CVE ID : CVE-2021-3006	N/A	A-SEA-SEAL-210121/241
seon-barton					
elementor_contact_form_db					
Cross-Site Request Forgery (CSRF)	12-Jan-21	6.8	The Elementor Contact Form DB plugin before 1.6 for WordPress allows CSRF via backend admin pages. CVE ID : CVE-2021-3133	https://plugins.trac.wordpress.org/changeset/2454670/	A-SEO-ELEM-210121/242
Seopanel					
seo_panel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jan-21	4.3	Seo Panel 4.8.0 allows reflected XSS via the seo/seopanel/login.php?sec=forgot email parameter. CVE ID : CVE-2021-3002	N/A	A-SEO-SEO_-210121/243
Snort					
snort					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-	A-SNO-SNOR-210121/244

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			<p>HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1223</p>	filepolbypass-67DEwMe2						
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	A-SNO-SNOR-210121/245					
Always-	13-Jan-21	5	Multiple Cisco products are	https://tools	A-SNO-SNOR-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Control Flow Implementation			affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network. CVE ID : CVE-2021-1236	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	210121/246

spring-boot-actuator-logview_project

spring-boot-actuator-logview

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jan-21	4	spring-boot-actuator-logview in a library that adds a simple logfile viewer as spring boot actuator endpoint. It is maven package "eu.hinsch:spring-boot-actuator-logview". In spring-boot-actuator-logview before version 0.2.13 there is a directory traversal vulnerability. The nature of this library is to expose a log file directory via admin (spring boot actuator) HTTP endpoints. Both the filename to view and a base folder (relative to the logging folder root) can be	https://github.com/lukashinsch/spring-boot-actuator-logview/commit/1c76e1ec3588c9f39e1a94bf27b5ff56eb8b17d6, https://github.com/lukashinsch/spring-boot-actuator-logview/commit/760ac	A-SPR-SPRI-210121/247
--	-----------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>specified via request parameters. While the filename parameter was checked to prevent directory traversal exploits (so that `filename=../somefile` would not work), the base folder parameter was not sufficiently checked, so that `filename=somefile&base=../` could access a file outside the logging base directory). The vulnerability has been patched in release 0.2.13. Any users of 0.2.12 should be able to update without any issues as there are no other changes in that release. There is no workaround to fix the vulnerability other than updating or removing the dependency. However, removing read access of the user the application is run with to any directory not required for running the application can limit the impact. Additionally, access to the logview endpoint can be limited by deploying the application behind a reverse proxy.</p> <p>CVE ID : CVE-2021-21234</p>	bb939a8d1f7d1a7dfcd51ca848eea04e772	

stableyieldcredit_project

stableyieldcredit

Incorrect Calculation	03-Jan-21	5	The _deposit function in the smart contract implementation for Stable Yield Credit (yCREDIT), an	N/A	A-STA-STAB-210121/248
-----------------------	-----------	---	--	-----	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Ethereum token, has certain incorrect calculations. An attacker can obtain more yCREDIT tokens than they should. CVE ID : CVE-2021-3004		
sudo_project					
sudo					
Improper Link Resolution Before File Access ('Link Following')	12-Jan-21	1.9	The sudoedit personality of Sudo before 1.9.5 may allow a local unprivileged user to perform arbitrary directory-existence tests by winning a sudo_edit.c race condition in replacing a user-controlled directory by a symlink to an arbitrary path. CVE ID : CVE-2021-23239	https://www.sudo.ws/table.html#1.9.5	A-SUD-SUDO-210121/249
Improper Link Resolution Before File Access ('Link Following')	12-Jan-21	4.4	selinux_edit_copy_tfiles in sudoedit in Sudo before 1.9.5 allows a local unprivileged user to gain file ownership and escalate privileges by replacing a temporary file with a symlink to an arbitrary file target. This affects SELinux RBAC support in permissive mode. Machines without SELinux are not vulnerable. CVE ID : CVE-2021-23240	https://bugzilla.suse.com/show_bug.cgi?id=CVE-2021-23240 , https://www.sudo.ws/table.html#1.9.5	A-SUD-SUDO-210121/250
Zend					
zend_framework					
Deserialization of Untrusted Data	04-Jan-21	7.5	** DISPUTED ** Laminas Project laminas-http before 2.14.2, and Zend Framework 3.0.0, has a deserialization vulnerability that can lead to	https://github.com/laminas/laminas-http/commit	A-ZEN-ZEND-210121/251

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote code execution if the content is controllable, related to the __destruct method of the Zend\Http\Response\Stream class in Stream.php. NOTE: Zend Framework is no longer supported by the maintainer. NOTE: the laminas-http vendor considers this a "vulnerability in the PHP language itself" but has added certain type checking as a way to prevent exploitation in (unrecommended) use cases where attacker-supplied data can be deserialized. CVE ID : CVE-2021-3007	s/2.15.x/src/Response/Stream.php, https://github.com/laminas/laminas-http/pull/48	

Operating System

Apple

mac_os

Heap-based Buffer Overflow	13-Jan-21	6.8	Adobe Photoshop version 22.1 (and earlier) is affected by a heap buffer overflow vulnerability when handling a specially crafted font file. Successful exploitation could lead to arbitrary code execution. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21006	https://helpx.adobe.com/security/products/photoshop/apsb21-01.html	O-APP-MAC_210121/252
----------------------------	-----------	-----	---	---	----------------------

Cisco

meraki_mx64_firmware

Improper	13-Jan-21	5	Multiple Cisco products are	https://tools	O-CIS-MERA-
----------	-----------	---	-----------------------------	---	-------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			<p>affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	210121/253

meraki_mx64w_firmware

Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes</p>	O-CIS-MERA-210121/254
-------------------------------	-----------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224		
meraki_mx67_firmware					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	O-CIS-MERA-210121/255

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
meraki_mx67c_firmware					
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	O-CIS-MERA-210121/256
meraki_mx67w_firmware					
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	O-CIS-MERA-210121/257

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>		

meraki_mx68_firmware

Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes</p>	O-CIS-MERA-210121/258
-------------------------------	-----------	---	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1224		
meraki_mx68cw_firmware					
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes</p>	O-CIS-MERA-210121/259
meraki_mx68w_firmware					
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes</p>	O-CIS-MERA-210121/260

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>		

meraki_mx100_firmware

Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes</p>	O-CIS-MERA-210121/261
-------------------------------	-----------	---	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224		
meraki_mx84_firmware					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	O-CIS-MERA-210121/262
meraki_mx250_firmware					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-	O-CIS-MERA-210121/263

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	MmzZrtes	

meraki_mx450_firmware

Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes</p>	O-CIS-MERA-210121/264
-------------------------------	-----------	---	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224		
rv130_firmware					
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/265

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			vulnerabilities. CVE ID : CVE-2021-1179							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1180	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/266					
Out-of-bounds	13-Jan-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	O-CIS-RV13-210121/267					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			<p>interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1181</p>	<p>ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/268

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1182</p>	sco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/269

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1183</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/270

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1190</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/271

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1191</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV13-210121/272

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1200</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/273

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1201</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/274

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1202</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/275

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			vulnerabilities. CVE ID : CVE-2021-1203							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1204	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/276					
Out-of-bounds	13-Jan-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	O-CIS-RV13-210121/277					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			<p>interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1205</p>	<p>security/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	

rv110w_wireless-n_vpn_firewall_firmware

Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV11-210121/278
------------------------	-----------	---	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1217</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
rv130_vpn_router_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-	O-CIS-RV13-210121/279

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1146</p>	inject-LBdQ2KRN	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	O-CIS-RV13-210121/280

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1147</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	0-CIS-RV13-210121/281

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1148</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1149</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	O-CIS-RV13-210121/282

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1150	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	O-CIS-RV13-210121/283
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-	O-CIS-RV13-210121/284

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1151</p>	LPTQ3EQC	
<p>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</p>	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	0-CIS-RV13-210121/285

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1152</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV13-210121/286

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			device. CVE ID : CVE-2021-1153							
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1154	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	O-CIS-RV13-210121/287					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-	O-CIS-RV13-210121/288					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1155</p>	LPTQ3EQC	
<p>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</p>	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	0-CIS-RV13-210121/289

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1156</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV13-210121/290

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. CVE ID : CVE-2021-1157		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1158	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	O-CIS-RV13-210121/291
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	O-CIS-RV13-210121/292

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1159	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/293

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1160</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV13-210121/294

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1161</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV13-210121/295

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1162		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV13-210121/296

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1163</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/297

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1164</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/298

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1165		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1166	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/299

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1167</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/300
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	O-CIS-RV13-210121/301

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1168</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-</p>	O-CIS-RV13-210121/302

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1169	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/303

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1170</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV13-210121/304

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1171</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV13-210121/305

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1172</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV13-210121/306

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1173</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/307

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1174</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/308

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1175		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1176	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/309

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1177</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/310
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	O-CIS-RV13-210121/311

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1178</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	O-CIS-RV13-210121/312

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1184	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/313

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1185</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV13-210121/314

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1186</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV13-210121/315

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1187</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV13-210121/316

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1188</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/317

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1189</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/318

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1192		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1193	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/319

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1194</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/320
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	O-CIS-RV13-210121/321

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1195</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	O-CIS-RV13-210121/322

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1196	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/323

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1197</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV13-210121/324

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1198</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV13-210121/325

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1199</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV13-210121/326

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1206</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/327

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1207</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/328

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1208		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1209	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/329

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1210</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/330
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	O-CIS-RV13-210121/331

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1211</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	O-CIS-RV13-210121/332

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1212	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/333

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1213</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV13-210121/334

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1214</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV13-210121/335

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1215		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV13-210121/336

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1216</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/337

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1217</p>		
rv130w_wireless-n_multifunction_vpn_router_firmware					
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/338

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1217		
rv215w_wireless-n_vpn_router_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1146	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	O-CIS-RV21-210121/339
Improper	13-Jan-21	9	Multiple vulnerabilities in	https://tools	O-CIS-RV21-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1147</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	210121/340
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-	O-CIS-RV21-210121/341

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1148</p>	LBdQ2KRN	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	O-CIS-RV21-210121/342

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1149		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	O-CIS-RV21-210121/343

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1150		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1151	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	O-CIS-RV21-210121/344
Improper Neutralization of Input	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	O-CIS-RV21-210121/345

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1152</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	O-CIS-RV21-210121/346

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1153</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV21-210121/347

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1154		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1155	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	O-CIS-RV21-210121/348
Improper Neutralization of Input	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	O-CIS-RV21-210121/349

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1156</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	O-CIS-RV21-210121/350

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1157</p>		
<p>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</p>	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	0-CIS-RV21-210121/351

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1158</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/352

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			that address these vulnerabilities. CVE ID : CVE-2021-1159							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1160	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV21-210121/353					
Out-of-	13-Jan-21	9	Multiple vulnerabilities in	https://tools	O-CIS-RV21-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1161</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/354
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV21-210121/355

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1162</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV21-210121/356

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1163</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/357

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1164</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/358

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1165</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/359

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1166</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/360

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1167</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/361

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1168</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/362

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			that address these vulnerabilities. CVE ID : CVE-2021-1169							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1170	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV21-210121/363					
Out-of-	13-Jan-21	9	Multiple vulnerabilities in	https://tools	O-CIS-RV21-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1171</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/364
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV21-210121/365

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1172</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV21-210121/366

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1173</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/367

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1174</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/368

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1175</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/369

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1176</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/370

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1177</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/371

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1178</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/372

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			that address these vulnerabilities. CVE ID : CVE-2021-1184							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1185	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV21-210121/373					
Out-of-	13-Jan-21	9	Multiple vulnerabilities in	https://tools	O-CIS-RV21-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1186</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/374
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV21-210121/375

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1187</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV21-210121/376

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1188</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/377

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1189</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/378

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1192</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/379

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1193</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/380

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1194</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/381

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1195</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/382

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			that address these vulnerabilities. CVE ID : CVE-2021-1196							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1197	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV21-210121/383					
Out-of-	13-Jan-21	9	Multiple vulnerabilities in	https://tools	O-CIS-RV21-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1198</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/384
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV21-210121/385

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1199</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV21-210121/386

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1206</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/387

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1207</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/388

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1208</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/389

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1209</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/390

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1210</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/391

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1211</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/392

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			that address these vulnerabilities. CVE ID : CVE-2021-1212							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1213	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV21-210121/393					
Out-of-	13-Jan-21	9	Multiple vulnerabilities in	https://tools	O-CIS-RV21-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1214</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/394
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV21-210121/395

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1215</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV21-210121/396

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1216</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV21-210121/397

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1217</p>		

rv110w_firmware

Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	0-CIS-RV11-210121/398
---	-----------	---	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1146</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	O-CIS-RV11-210121/399

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1147</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1148</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	O-CIS-RV11-210121/400

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1149	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	O-CIS-RV11-210121/401
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-	O-CIS-RV11-210121/402

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1150</p>	inject-LBdQ2KRN	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV11-210121/403

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1151</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV11-210121/404

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1152</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1153</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV11-210121/405
Improper Neutralization of Input During Web Page Generation	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV11-210121/406

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			<p>authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1154</p>	sco-sa-rv-stored-xss-LPTQ3EQC	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV11-210121/407

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1155</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV11-210121/408

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1156</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1157</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV11-210121/409
Improper Neutralization of Input During Web Page Generation	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV11-210121/410

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			<p>authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1158</p>	sco-sa-rv-stored-xss-LPTQ3EQC	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV11-210121/411

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1159</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV11-210121/412

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1160</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV11-210121/413

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1161</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/414

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1162</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/415

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1163		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1164	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV11-210121/416

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1165</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/417
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	O-CIS-RV11-210121/418

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1166</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	O-CIS-RV11-210121/419

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1167	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV11-210121/420

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1168</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV11-210121/421

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1169</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV11-210121/422

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1170		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	O-CIS-RV11-210121/423

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1171</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/424

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1172</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/425

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1173		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1174	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV11-210121/426

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1175</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/427
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	O-CIS-RV11-210121/428

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1176</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	O-CIS-RV11-210121/429

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1177	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV11-210121/430

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1178</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV11-210121/431

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1179</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV11-210121/432

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1180</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV11-210121/433

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1181</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/434

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1182</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/435

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1183		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1184	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV11-210121/436

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1185</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/437
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	O-CIS-RV11-210121/438

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1186</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-</p>	O-CIS-RV11-210121/439

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1187	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV11-210121/440

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1188</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV11-210121/441

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1189</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV11-210121/442

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1190</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV11-210121/443

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1191</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/444

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1192</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/445

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1193		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1194	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV11-210121/446

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1195</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/447
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	O-CIS-RV11-210121/448

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1196</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	O-CIS-RV11-210121/449

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1197	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV11-210121/450

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1198</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV11-210121/451

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1199</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV11-210121/452

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1200</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV11-210121/453

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1201</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/454

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1202</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/455

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1203		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1204	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV11-210121/456

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1205</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/457
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	O-CIS-RV11-210121/458

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1206</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	O-CIS-RV11-210121/459

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1207	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV11-210121/460

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1208</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV11-210121/461

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1209</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV11-210121/462

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1210</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	O-CIS-RV11-210121/463

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1211</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/464

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1212</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/465

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1213		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1214	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV11-210121/466

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1215</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV11-210121/467
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	O-CIS-RV11-210121/468

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1216</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	

rv130w_firmware

Improper Neutralization of Special Elements used in a Command ('Command	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-</p>	O-CIS-RV13-210121/469
---	-----------	---	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			<p>attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1146</p>	command-inject-LBdQ2KRN	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	O-CIS-RV13-210121/470

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1147</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	O-CIS-RV13-210121/471

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1148		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	O-CIS-RV13-210121/472

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1149		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	O-CIS-RV13-210121/473
Improper Neutralization of Input During Web Page Generation ('Cross-site	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV13-210121/474

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			<p>attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1151</p>	stored-xss-LPTQ3EQC	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV13-210121/475

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1152</p>		
<p>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</p>	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV13-210121/476

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials on the affected device. CVE ID : CVE-2021-1153		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1154	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	O-CIS-RV13-210121/477
Improper Neutralization of Input During Web Page Generation ('Cross-site	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV13-210121/478

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1155	stored-xss-LPTQ3EQC	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	O-CIS-RV13-210121/479

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1156</p>		
<p>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</p>	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	O-CIS-RV13-210121/480

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials on the affected device. CVE ID : CVE-2021-1157		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1158	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	O-CIS-RV13-210121/481
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV13-210121/482

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1159</p>	overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/483

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1160</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/484

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1161</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV13-210121/485

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1162</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/486

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1163</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/487

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1164</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/488

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1165		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/489

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1166		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1167</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/490
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	O-CIS-RV13-210121/491

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1168</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV13-210121/492

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1169</p>	overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/493

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1170</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/494

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1171</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/495

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1172</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/496

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1173		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/497

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1174</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/498

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1175		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/499

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1176		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1177</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/500
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	O-CIS-RV13-210121/501

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1178</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/502

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1179</p>	overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/503

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1180</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/504

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1181</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/505

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1182</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/506

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1183</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/507

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1184</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/508

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1185		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/509

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1186		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1187</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/510
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	O-CIS-RV13-210121/511

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1188</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/512

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1189</p>	overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/513

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1190</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/514

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1191</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/515

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1192</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/516

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1193</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/517

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1194</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/518

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1195		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/519

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1196		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1197</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/520
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	O-CIS-RV13-210121/521

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1198</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/522

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1199</p>	overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/523

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1200</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/524

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1201</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV13-210121/525

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1202</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/526

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1203</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/527

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1204</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/528

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1205		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/529

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1206		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1207</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/530
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	O-CIS-RV13-210121/531

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1208</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV13-210121/532

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1209</p>	overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/533

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1210</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/534

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1211</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV13-210121/535

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1212</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/536

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1213</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/537

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1214</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV13-210121/538

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1215		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV13-210121/539

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1216		
rv215w_firmware					
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1179</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV21-210121/540
Out-of-bounds	13-Jan-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	O-CIS-RV21-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			<p>interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1180</p>	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/541
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV21-210121/542

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1181</p>	sco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV21-210121/543

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1182</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/544

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1183</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/545

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1190</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	0-CIS-RV21-210121/546

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1191</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/547

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1200</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/548

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1201</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/549

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			vulnerabilities. CVE ID : CVE-2021-1202							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1203	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	O-CIS-RV21-210121/550					
Out-of-bounds	13-Jan-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	O-CIS-RV21-210121/551					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			<p>interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1204</p>	<p>ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	O-CIS-RV21-210121/552

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1205</p>	sco-sa-rv-overflow-WUnUgv4U	

ios_xe

Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-</p>	0-CIS-IOS_-210121/553
-------------------------------	-----------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1223</p>	67DEwMe2	
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	O-CIS-IOS_-210121/554
Always-Incorrect Control Flow	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort application</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	O-CIS-IOS_-210121/555

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Implementation			<p>detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network.</p> <p>CVE ID : CVE-2021-1236</p>	er/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	

Citrix hypervisor

Allocation of Resources Without Limits or Throttling	08-Jan-21	4.6	<p>NVIDIA Virtual GPU Manager NVIDIA vGPU manager contains a vulnerability in the vGPU plugin in which it allows guests to allocate some resources for which the guest is not authorized, which may lead to integrity and confidentiality loss, denial of service, or information disclosure. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).</p> <p>CVE ID : CVE-2021-1057</p>	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-CIT-HYPE-210121/556
Improper Input Validation	08-Jan-21	3.6	<p>NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an</p>	https://nvidia.custhelp.com/app/answers/detail/	O-CIT-HYPE-210121/557

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input data size is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1058	a_id/5142	
Integer Overflow or Wraparound	08-Jan-21	4.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input index is not validated, which may lead to integer overflow, which in turn may cause tampering of data, information disclosure, or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1059	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-CIT-HYPE-210121/558
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input index is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1060	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-CIT-HYPE-210121/559
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	08-Jan-21	3.3	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which a race condition may cause the vGPU plugin to continue using a previously validated resource that has since changed, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-CIT-HYPE-210121/560

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			denial of service or information disclosure. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1061		
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input data length is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1062	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-CIT-HYPE-210121/561
Out-of-bounds Read	08-Jan-21	4.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input offset is not validated, which may lead to a buffer overread, which in turn may cause tampering of data, information disclosure, or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1063	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-CIT-HYPE-210121/562
NULL Pointer Dereference	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which it obtains a value from an untrusted source, converts this value to a pointer, and dereferences the resulting pointer, which may lead to information disclosure or denial of service. This affects	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-CIT-HYPE-210121/563

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1064		
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which input data is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1065	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-CIT-HYPE-210121/564
Uncontrolled Resource Consumption	08-Jan-21	2.1	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which input data is not validated, which may lead to unexpected consumption of resources, which in turn may lead to denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1066	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-CIT-HYPE-210121/565
Google					
android					
Out-of-bounds Write	11-Jan-21	4.6	In gedit, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android SoC; Android ID: A-	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/566

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			172514667. CVE ID : CVE-2021-0301		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jan-21	6.9	In dispatchGraphTerminationMessage() of packages/services/Car/computepipe/runner/graph/StreamSetObserver.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Android ID: A-170407229. CVE ID : CVE-2021-0303	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/567
Improper Privilege Management	11-Jan-21	4.9	In several functions of GlobalScreenshot.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure of the user's contacts with User execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-10, Android-8.0, Android-8.1, Android-9; Android ID: A-162738636. CVE ID : CVE-2021-0304	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/568
Improper Privilege Management	11-Jan-21	7.2	In addAllPermissions of PermissionManagerService.java, there is a possible permissions bypass when	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/569

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			<p>upgrading major Android versions which allows an app to gain the android.permission.ACTIVITY_RECOGNITION permission without user confirmation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11, Android-8.0, Android-8.1, Android-9, Android-10; Android ID: A-154505240.</p> <p>CVE ID : CVE-2021-0306</p>	21-01-01						
Not Available	11-Jan-21	7.2	<p>In updatePermissionSourcePackage of PermissionManagerService.java, there is a possible automatic runtime permission grant due to a confused deputy. This could lead to local escalation of privilege allowing a malicious app to silently gain access to a dangerous permission with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-10, Android-11; Android ID: A-155648771.</p> <p>CVE ID : CVE-2021-0307</p>	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/570					
Out-of-bounds	11-Jan-21	7.2	<p>In ReadLogicalParts of basicmbr.cc, there is a</p>	https://source.android.c	O-GOO-ANDR-210121/571					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-8.1, Android-9, Android-10, Android-11, Android-8.0; Android ID: A-158063095. CVE ID : CVE-2021-0308	om/security/bulletin/2021-01-01	
Not Available	11-Jan-21	4.9	In onCreate of grantCredentialsPermission Activity, there is a confused deputy. This could lead to local information disclosure and account access with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-8.1, Android-9, Android-10, Android-11, Android-8.0; Android ID: A-158480899. CVE ID : CVE-2021-0309	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/572
Use After Free	11-Jan-21	7.2	In LazyServiceRegistrar of LazyServiceRegistrar.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Android ID: A-	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/573

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			170212632. CVE ID : CVE-2021-0310		
Out-of-bounds Write	11-Jan-21	7.1	In ElementaryStreamQueue::dequeueAccessUnitH264() of ESQueue.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-9, Android-10, Android-11, Android-8.0, Android-8.1; Android ID: A-170240631. CVE ID : CVE-2021-0311	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/574
Out-of-bounds Write	11-Jan-21	7.1	In WAVSource::read of WAVExtractor.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-8.1, Android-9, Android-10, Android-11, Android-8.0; Android ID: A-170583712. CVE ID : CVE-2021-0312	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/575
Improper Input Validation	11-Jan-21	7.8	In isWordBreakAfter of LayoutUtils.cpp, there is a possible way to slow or crash a TextView due to improper input validation.	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/576

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-9, Android-10, Android-11, Android-8.0, Android-8.1; Android ID: A-170968514. CVE ID : CVE-2021-0313		
Improper Restriction of Rendered UI Layers or Frames	11-Jan-21	4.4	In onCreate of GrantCredentialsPermission Activity.java, there is a possible way to convince the user to grant an app access to an account due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-8.1, Android-9, Android-10, Android-11, Android-8.0; Android ID: A-169763814. CVE ID : CVE-2021-0315	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/577
Out-of-bounds Write	11-Jan-21	10	In avrc_pars_vendor_cmd of avrc_pars_tg.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions:	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/578

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Android-11, Android-8.0, Android-8.1, Android-9, Android-10; Android ID: A-168802990. CVE ID : CVE-2021-0316		
Improper Privilege Management	11-Jan-21	4.4	In createOrUpdate of Permission.java and related code, there is possible permission escalation due to a logic error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-10, Android-11, Android-8.0, Android-8.1, Android-9; Android ID: A-168319670. CVE ID : CVE-2021-0317	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/579
Out-of-bounds Write	11-Jan-21	7.2	In appendEventsToCacheLocked of SensorEventConnection.cpp, there is a possible out of bounds write due to a use-after-free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-9, Android-8.1, Android-10, Android-11; Android ID: A-168211968. CVE ID : CVE-2021-0318	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/580
Incorrect Authorization	11-Jan-21	4.4	In checkCallerIsSystemOr of CompanionDeviceManagerS	https://source.android.c	O-GOO-ANDR-210121/581

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
n			ervice.java, there is a possible way to get a nearby Bluetooth device's MAC address without appropriate permissions due to a permissions bypass. This could lead to local escalation of privilege that grants access to nearby MAC addresses, with User execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-8.0, Android-8.1, Android-9, Android-10, Android-11; Android ID: A-167244818. CVE ID : CVE-2021-0319	om/security/bulletin/2021-01-01						
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jan-21	1.9	In is_device_locked and set_device_locked of keystore_keymaster_enforcement.h, there is a possible bypass of lockscreen requirements for keyguard bound keys due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-10, Android-11; Android ID: A-169933423. CVE ID : CVE-2021-0320	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/582					
Exposure of Sensitive Information to an Unauthorized	11-Jan-21	2.1	In enforceDumpPermissionForPackage of ActivityManagerService.java, there is a possible way to	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/583					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Actor			determine if a package is installed due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Android ID: A-166667403. CVE ID : CVE-2021-0321		
Improper Input Validation	11-Jan-21	1.9	In onCreate of SlicePermissionActivity.java, there is a possible misleading string displayed due to improper input validation. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-10, Android-11, Android-9; Android ID: A-159145361. CVE ID : CVE-2021-0322	https://source.android.com/security/bulletin/2021-01-01	O-GOO-ANDR-210121/584
Use After Free	11-Jan-21	4.6	In tun_get_user of tun.c, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges required. User interaction is not required for exploitation. Product: Android; Versions: Android kernel; Android ID: A-146554327.	https://source.android.com/security/bulletin/pixel/2021-01-01	O-GOO-ANDR-210121/585

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0342		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-21	5.8	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Broadcom Bluetooth chipsets) software. The Bluetooth UART driver has a buffer overflow. The Samsung ID is SVE-2020-18731 (January 2021). CVE ID : CVE-2021-22492	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-210121/586
Out-of-bounds Write	05-Jan-21	6.8	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. The quram library allows attackers to execute arbitrary code or cause a denial of service (memory corruption) during dng decoding. The Samsung ID is SVE-2020-18811 (January 2021). CVE ID : CVE-2021-22493	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-210121/587
Not Available	05-Jan-21	4.3	An issue was discovered in the fingerprint scanner on Samsung Note20 mobile devices with Q(10.0) software. When a screen protector is used, the required image compensation is not present. Consequently, inversion can occur during fingerprint enrollment, and a high False Recognition Rate (FRR) can occur. The Samsung ID is SVE-2020-19216 (January 2021).	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-210121/588

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22494		
Out-of-bounds Write	05-Jan-21	7.1	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), Q(10.0), and R(11.0) (Exynos chipsets) software. The Mali GPU driver allows out-of-bounds access and a device reset. The Samsung ID is SVE-2020-19174 (January 2021). CVE ID : CVE-2021-22495	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-210121/589
Not Available	05-Jan-21	2.1	An issue was discovered on LG mobile devices with Android OS 10 software. There was no write protection for the MTK protect2 partition. The LG ID is LVE-SMP-200028 (January 2021). CVE ID : CVE-2021-3022	https://lgsecurity.lge.com/	O-GOO-ANDR-210121/590

Linux

linux_kernel

Improper Privilege Management	08-Jan-21	7.2	NVIDIA GPU Display Driver for Windows and Linux, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape or IOCTL in which user-mode clients can access legacy privileged APIs, which may lead to denial of service, escalation of privileges, and information disclosure. CVE ID : CVE-2021-1052	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-LIN-LINU-210121/591
Improper Input	08-Jan-21	2.1	NVIDIA GPU Display Driver for Windows and Linux, all	https://nvidia.custhelp.com/	O-LIN-LINU-210121/592

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape or IOCTL in which improper validation of a user pointer may lead to denial of service. CVE ID : CVE-2021-1053	om/app/answers/detail/a_id/5142	
Incorrect Default Permissions	08-Jan-21	3.6	NVIDIA GPU Display Driver for Linux, all versions, contains a vulnerability in the kernel mode layer (nvidia.ko) in which it does not completely honor operating system file system permissions to provide GPU device-level isolation, which may lead to denial of service or information disclosure. CVE ID : CVE-2021-1056	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-LIN-LINU-210121/593
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input data size is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1058	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-LIN-LINU-210121/594
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input index is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-LIN-LINU-210121/595

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			(prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1060							
Use After Free	08-Jan-21	6.8	Use after free in drag and drop in Google Chrome on Linux prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21107	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html , https://crbug.com/1153595	O-LIN-LINU-210121/596					
mercusys										
mercury_x18g_firmware										
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jan-21	5	MERCUSYS Mercury X18G 1.0.5 devices allow Directory Traversal via ../ in conjunction with a loginLess or login.htm URI (for authentication bypass) to the web server, as demonstrated by the /loginLess/../../etc/passwd URI. CVE ID : CVE-2021-23241	https://www.mercurycom.cn/product-521-1.html , https://www.mercusys.com/en/	O-MER-MERC-210121/597					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jan-21	5	MERCUSYS Mercury X18G 1.0.5 devices allow Directory Traversal via ../ to the UPnP server, as demonstrated by the ../../conf/template/uhttpd.json URI. CVE ID : CVE-2021-23242	https://www.mercurycom.cn/product-521-1.html , https://www.mercusys.com/en/	O-MER-MERC-210121/598					
Microsoft										
windows										
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	08-Jan-21	7.2	NVIDIA GPU Display Driver for Windows, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which an operation is performed which may lead to denial of service or escalation of privileges. CVE ID : CVE-2021-1051	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-MIC-WIND-210121/599
Improper Privilege Management	08-Jan-21	7.2	NVIDIA GPU Display Driver for Windows and Linux, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape or IOCTL in which user-mode clients can access legacy privileged APIs, which may lead to denial of service, escalation of privileges, and information disclosure. CVE ID : CVE-2021-1052	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-MIC-WIND-210121/600
Improper Input Validation	08-Jan-21	2.1	NVIDIA GPU Display Driver for Windows and Linux, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape or IOCTL in which improper validation of a user pointer may lead to denial of service. CVE ID : CVE-2021-1053	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-MIC-WIND-210121/601
Incorrect Authorization	08-Jan-21	2.1	NVIDIA GPU Display Driver for Windows, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-MIC-WIND-210121/602

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DxgkDdiEscape in which the software does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action, which may lead to denial of service. CVE ID : CVE-2021-1054		
Incorrect Authorization	08-Jan-21	4.6	NVIDIA GPU Display Driver for Windows, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which improper access control may lead to denial of service and information disclosure. CVE ID : CVE-2021-1055	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-MIC-WIND-210121/603
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input data size is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1058	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-MIC-WIND-210121/604
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input index is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-MIC-WIND-210121/605

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			11.0 (prior to 11.3). CVE ID : CVE-2021-1060							
Heap-based Buffer Overflow	13-Jan-21	6.8	Adobe Photoshop version 22.1 (and earlier) is affected by a heap buffer overflow vulnerability when handling a specially crafted font file. Successful exploitation could lead to arbitrary code execution. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21006	https://helpx.adobe.com/security/products/photoshop/apsb21-01.html	O-MIC-WIND-210121/606					
Uncontrolled Search Path Element	13-Jan-21	6.8	Adobe Illustrator version 25.0 (and earlier) is affected by an uncontrolled search path element 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-2021-21007	https://helpx.adobe.com/security/products/illustrator/apsb21-02.html	O-MIC-WIND-210121/607					
Uncontrolled Search Path Element	13-Jan-21	6.8	Adobe Animate version 21.0 (and earlier) is affected by an uncontrolled search path element 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-2021-21008	https://helpx.adobe.com/security/products/animate/apsb21-03.html	O-MIC-WIND-210121/608					
Uncontrolled Search Path	13-Jan-21	5.1	InCopy version 15.1.1 (and earlier) for Windows is	https://helpx.adobe.com	O-MIC-WIND-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Element			affected by an uncontrolled search path 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-2021-21010	/security/products/inco py/apsb21- 05.html	210121/609
Uncontrolled Search Path Element	13-Jan-21	5.1	Adobe Captivate 2019 version 11.5.1.499 (and earlier) is affected by an uncontrolled search path element vulnerability that could lead to privilege escalation. An attacker with permissions to write to the file system could leverage this vulnerability to escalate privileges. CVE ID : CVE-2021-21011	https://helpx.adobe.com/security/products/captivate/apsb21-06.html	O-MIC-WIND-210121/610
Out-of-bounds Write	13-Jan-21	6.8	Adobe Bridge version 11.0 (and earlier) is affected by an out-of-bounds write vulnerability when parsing TTF files 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-2021-21012	https://helpx.adobe.com/security/products/bridge/apsb21-07.html	O-MIC-WIND-210121/611
Out-of-bounds Write	13-Jan-21	6.8	Adobe Bridge version 11.0 (and earlier) is affected by an out-of-bounds write vulnerability when parsing TTF files that could result in	https://helpx.adobe.com/security/products/bridge/apsb21-	O-MIC-WIND-210121/612

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21013	07.html	
windows_10					
Not Available	12-Jan-21	2.1	Windows DNS Query Information Disclosure Vulnerability CVE ID : CVE-2021-1637	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1637	O-MIC-WIND-210121/613
Incorrect Authorization	12-Jan-21	2.1	Windows Bluetooth Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-1683, CVE-2021-1684. CVE ID : CVE-2021-1638	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1638	O-MIC-WIND-210121/614
Improper Privilege Management	12-Jan-21	4.6	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1685. CVE ID : CVE-2021-1642	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1642	O-MIC-WIND-210121/615
Not Available	12-Jan-21	4.3	Windows Docker Information Disclosure Vulnerability CVE ID : CVE-2021-1645	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-210121/616

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-1645	
Improper Privilege Management	12-Jan-21	7.2	Windows WLAN Service Elevation of Privilege Vulnerability CVE ID : CVE-2021-1646	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1646	O-MIC-WIND-210121/617
Not Available	12-Jan-21	7.2	Microsoft Defender Remote Code Execution Vulnerability CVE ID : CVE-2021-1647	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1647	O-MIC-WIND-210121/618
Improper Privilege Management	12-Jan-21	7.2	Microsoft splwow64 Elevation of Privilege Vulnerability CVE ID : CVE-2021-1648	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1648	O-MIC-WIND-210121/619
Improper Privilege Management	12-Jan-21	7.2	Active Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1649	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1649	O-MIC-WIND-210121/620
Improper Privilege Management	12-Jan-21	7.2	Windows Runtime C++ Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1650	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1650	O-MIC-WIND-210121/621

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2021-1650	
Improper Privilege Management	12-Jan-21	9	Windows LUAFV Elevation of Privilege Vulnerability CVE ID : CVE-2021-1706	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1706	O-MIC-WIND-210121/622
Not Available	12-Jan-21	6.8	Microsoft Windows Media Foundation Remote Code Execution Vulnerability CVE ID : CVE-2021-1710	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1710	O-MIC-WIND-210121/623
Improper Privilege Management	12-Jan-21	7.2	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1680. CVE ID : CVE-2021-1651	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1651	O-MIC-WIND-210121/624
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1653, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1652	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1652	O-MIC-WIND-210121/625
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1652	O-MIC-WIND-210121/626

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			1652, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1653	US/security-guidance/advisory/CVE-2021-1653						
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1654	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1654	O-MIC-WIND-210121/627					
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1654, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1655	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1655	O-MIC-WIND-210121/628					
Not Available	12-Jan-21	2.1	TPM Device Driver Information Disclosure Vulnerability CVE ID : CVE-2021-1656	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1656	O-MIC-WIND-210121/629					
Improper Privilege Management	12-Jan-21	7.2	Windows Fax Compose Form Remote Code Execution Vulnerability CVE ID : CVE-2021-1657	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1657	O-MIC-WIND-210121/630					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jan-21	4.6	Windows Event Tracing Elevation of Privilege Vulnerability CVE ID : CVE-2021-1662	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1662	O-MIC-WIND-210121/631
Exposure of Sensitive Information to an Unauthorized Actor	12-Jan-21	2.1	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-1670, CVE-2021-1672. CVE ID : CVE-2021-1663	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1663	O-MIC-WIND-210121/632
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1666, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1664	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1664	O-MIC-WIND-210121/633
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1664, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1666	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1666	O-MIC-WIND-210121/634
windows_7					
Not Available	12-Jan-21	7.2	Microsoft Defender Remote	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1666	O-MIC-WIND-210121/635

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability CVE ID : CVE-2021-1647	oosoft.com/en-US/security-guidance/advisory/CVE-2021-1647	210121/635
Improper Privilege Management	12-Jan-21	7.2	Active Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1649	https://port al.ms rc.micr osoft.com/en-US/security-guidance/advisory/CVE-2021-1649	O-MIC-WIND-210121/636
Improper Privilege Management	12-Jan-21	9	Windows LUA FV Elevation of Privilege Vulnerability CVE ID : CVE-2021-1706	https://port al.ms rc.micr osoft.com/en-US/security-guidance/advisory/CVE-2021-1706	O-MIC-WIND-210121/637
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1653, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1652	https://port al.ms rc.micr osoft.com/en-US/security-guidance/advisory/CVE-2021-1652	O-MIC-WIND-210121/638
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693.	https://port al.ms rc.micr osoft.com/en-US/security-guidance/advisory/CVE-2021-1653	O-MIC-WIND-210121/639

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1653		
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1654	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1654	O-MIC-WIND-210121/640
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1654, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1655	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1655	O-MIC-WIND-210121/641
Not Available	12-Jan-21	2.1	TPM Device Driver Information Disclosure Vulnerability CVE ID : CVE-2021-1656	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1656	O-MIC-WIND-210121/642
Improper Privilege Management	12-Jan-21	7.2	Windows Fax Compose Form Remote Code Execution Vulnerability CVE ID : CVE-2021-1657	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1657	O-MIC-WIND-210121/643
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1657	O-MIC-WIND-210121/644

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-1658, CVE-2021-1660, CVE-2021-1666, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1664	US/security-guidance/advisory/CVE-2021-1664	
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1664, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1666	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1666	O-MIC-WIND-210121/645

windows_8.1

Not Available	12-Jan-21	2.1	Windows DNS Query Information Disclosure Vulnerability CVE ID : CVE-2021-1637	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1637	O-MIC-WIND-210121/646
Not Available	12-Jan-21	7.2	Microsoft Defender Remote Code Execution Vulnerability CVE ID : CVE-2021-1647	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1647	O-MIC-WIND-210121/647
Improper Privilege Management	12-Jan-21	7.2	Microsoft splwow64 Elevation of Privilege Vulnerability CVE ID : CVE-2021-1648	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1648	O-MIC-WIND-210121/648

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2021-1648	
Improper Privilege Management	12-Jan-21	7.2	Active Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1649	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1649	O-MIC-WIND-210121/649
Improper Privilege Management	12-Jan-21	7.2	Windows Runtime C++ Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1650	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1650	O-MIC-WIND-210121/650
Improper Privilege Management	12-Jan-21	9	Windows LUAFV Elevation of Privilege Vulnerability CVE ID : CVE-2021-1706	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1706	O-MIC-WIND-210121/651
Not Available	12-Jan-21	6.8	Microsoft Windows Media Foundation Remote Code Execution Vulnerability CVE ID : CVE-2021-1710	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1710	O-MIC-WIND-210121/652
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1653, CVE-2021-1654, CVE-	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210121/653

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1652	guidance/advisory/CVE-2021-1652	
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1653	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1653	O-MIC-WIND-210121/654
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1654	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1654	O-MIC-WIND-210121/655
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1654, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1655	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1655	O-MIC-WIND-210121/656
Not Available	12-Jan-21	2.1	TPM Device Driver Information Disclosure Vulnerability CVE ID : CVE-2021-1656	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-210121/657

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-1656	
Improper Privilege Management	12-Jan-21	7.2	Windows Fax Compose Form Remote Code Execution Vulnerability CVE ID : CVE-2021-1657	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1657	O-MIC-WIND-210121/658
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1666, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1664	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1664	O-MIC-WIND-210121/659
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1664, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1666	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1666	O-MIC-WIND-210121/660
windows_rt_8.1					
Not Available	12-Jan-21	2.1	Windows DNS Query Information Disclosure Vulnerability CVE ID : CVE-2021-1637	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1637	O-MIC-WIND-210121/661

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	12-Jan-21	7.2	Microsoft Defender Remote Code Execution Vulnerability CVE ID : CVE-2021-1647	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1647	O-MIC-WIND-210121/662
Improper Privilege Management	12-Jan-21	7.2	Active Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1649	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1649	O-MIC-WIND-210121/663
Improper Privilege Management	12-Jan-21	7.2	Windows Runtime C++ Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1650	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1650	O-MIC-WIND-210121/664
Improper Privilege Management	12-Jan-21	9	Windows LUAFV Elevation of Privilege Vulnerability CVE ID : CVE-2021-1706	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1706	O-MIC-WIND-210121/665
Not Available	12-Jan-21	6.8	Microsoft Windows Media Foundation Remote Code Execution Vulnerability CVE ID : CVE-2021-1710	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1710	O-MIC-WIND-210121/666

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-1710	
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1653, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1652	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1652	O-MIC-WIND-210121/667
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1653	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1653	O-MIC-WIND-210121/668
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1654	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1654	O-MIC-WIND-210121/669
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1654, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1655	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1655	O-MIC-WIND-210121/670
Not Available	12-Jan-21	2.1	TPM Device Driver	https://port	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability CVE ID : CVE-2021-1656	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1656	210121/671
Improper Privilege Management	12-Jan-21	7.2	Windows Fax Compose Form Remote Code Execution Vulnerability CVE ID : CVE-2021-1657	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1657	O-MIC-WIND-210121/672
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1666, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1664	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1664	O-MIC-WIND-210121/673
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1664, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1666	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1666	O-MIC-WIND-210121/674
windows_server_2008					
Not Available	12-Jan-21	7.2	Microsoft Defender Remote Code Execution Vulnerability	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1675	O-MIC-WIND-210121/675

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1647	n-US/security-guidance/advisory/CVE-2021-1647	
Improper Privilege Management	12-Jan-21	7.2	Active Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1649	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1649	O-MIC-WIND-210121/676
Improper Privilege Management	12-Jan-21	9	Windows LUAFV Elevation of Privilege Vulnerability CVE ID : CVE-2021-1706	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1706	O-MIC-WIND-210121/677
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1653, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1652	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1652	O-MIC-WIND-210121/678
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1653	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1653	O-MIC-WIND-210121/679

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1654	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1654	O-MIC-WIND-210121/680
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1654, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1655	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1655	O-MIC-WIND-210121/681
Not Available	12-Jan-21	2.1	TPM Device Driver Information Disclosure Vulnerability CVE ID : CVE-2021-1656	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1656	O-MIC-WIND-210121/682
Improper Privilege Management	12-Jan-21	7.2	Windows Fax Compose Form Remote Code Execution Vulnerability CVE ID : CVE-2021-1657	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1657	O-MIC-WIND-210121/683
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660,	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210121/684

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-1666, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1664	guidance/advisory/CVE-2021-1664	
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1664, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1666	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1666	O-MIC-WIND-210121/685

windows_server_2012

Not Available	12-Jan-21	2.1	Windows DNS Query Information Disclosure Vulnerability CVE ID : CVE-2021-1637	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1637	O-MIC-WIND-210121/686
Not Available	12-Jan-21	7.2	Microsoft Defender Remote Code Execution Vulnerability CVE ID : CVE-2021-1647	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1647	O-MIC-WIND-210121/687
Improper Privilege Management	12-Jan-21	7.2	Microsoft splwow64 Elevation of Privilege Vulnerability CVE ID : CVE-2021-1648	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-210121/688

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-1648	
Improper Privilege Management	12-Jan-21	7.2	Active Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1649	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1649	O-MIC-WIND-210121/689
Improper Privilege Management	12-Jan-21	7.2	Windows Runtime C++ Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1650	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1650	O-MIC-WIND-210121/690
Improper Privilege Management	12-Jan-21	9	Windows LUAFV Elevation of Privilege Vulnerability CVE ID : CVE-2021-1706	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1706	O-MIC-WIND-210121/691
Not Available	12-Jan-21	6.8	Microsoft Windows Media Foundation Remote Code Execution Vulnerability CVE ID : CVE-2021-1710	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1710	O-MIC-WIND-210121/692
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1653, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659,	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-210121/693

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1652	visory/CVE-2021-1652	
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1653	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1653	O-MIC-WIND-210121/694
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1654	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1654	O-MIC-WIND-210121/695
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1654, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1655	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1655	O-MIC-WIND-210121/696
Not Available	12-Jan-21	2.1	TPM Device Driver Information Disclosure Vulnerability CVE ID : CVE-2021-1656	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1656	O-MIC-WIND-210121/697

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jan-21	7.2	Windows Fax Compose Form Remote Code Execution Vulnerability CVE ID : CVE-2021-1657	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1657	O-MIC-WIND-210121/698
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1666, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1664	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1664	O-MIC-WIND-210121/699
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1664, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1666	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1666	O-MIC-WIND-210121/700

windows_server_2016

Not Available	12-Jan-21	2.1	Windows DNS Query Information Disclosure Vulnerability CVE ID : CVE-2021-1637	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1637	O-MIC-WIND-210121/701
Incorrect Authorizatio	12-Jan-21	2.1	Windows Bluetooth Security Feature Bypass Vulnerability	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1637	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			This CVE ID is unique from CVE-2021-1683, CVE-2021-1684. CVE ID : CVE-2021-1638	osoft.com/en-US/security-guidance/advisory/CVE-2021-1638	210121/702
Improper Privilege Management	12-Jan-21	4.6	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1685. CVE ID : CVE-2021-1642	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1642	O-MIC-WIND-210121/703
Not Available	12-Jan-21	4.3	Windows Docker Information Disclosure Vulnerability CVE ID : CVE-2021-1645	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1645	O-MIC-WIND-210121/704
Improper Privilege Management	12-Jan-21	7.2	Windows WLAN Service Elevation of Privilege Vulnerability CVE ID : CVE-2021-1646	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1646	O-MIC-WIND-210121/705
Not Available	12-Jan-21	7.2	Microsoft Defender Remote Code Execution Vulnerability CVE ID : CVE-2021-1647	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1647	O-MIC-WIND-210121/706
Improper	12-Jan-21	7.2	Microsoft splwow64	https://port	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			Elevation of Privilege Vulnerability CVE ID : CVE-2021-1648	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1648	210121/707
Improper Privilege Management	12-Jan-21	7.2	Active Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1649	https://port.al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1649	O-MIC-WIND-210121/708
Improper Privilege Management	12-Jan-21	7.2	Windows Runtime C++ Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1650	https://port.al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1650	O-MIC-WIND-210121/709
Improper Privilege Management	12-Jan-21	9	Windows LUAFV Elevation of Privilege Vulnerability CVE ID : CVE-2021-1706	https://port.al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1706	O-MIC-WIND-210121/710
Not Available	12-Jan-21	6.8	Microsoft Windows Media Foundation Remote Code Execution Vulnerability CVE ID : CVE-2021-1710	https://port.al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1710	O-MIC-WIND-210121/711

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jan-21	7.2	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1680. CVE ID : CVE-2021-1651	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1651	O-MIC-WIND-210121/712
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1653, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1652	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1652	O-MIC-WIND-210121/713
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1653	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1653	O-MIC-WIND-210121/714
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1654	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1654	O-MIC-WIND-210121/715
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1654	O-MIC-WIND-210121/716

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1652, CVE-2021-1653, CVE-2021-1654, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1655	US/security-guidance/advisory/CVE-2021-1655	
Not Available	12-Jan-21	2.1	TPM Device Driver Information Disclosure Vulnerability CVE ID : CVE-2021-1656	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1656	O-MIC-WIND-210121/717
Improper Privilege Management	12-Jan-21	7.2	Windows Fax Compose Form Remote Code Execution Vulnerability CVE ID : CVE-2021-1657	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1657	O-MIC-WIND-210121/718
Improper Privilege Management	12-Jan-21	4.6	Windows Event Tracing Elevation of Privilege Vulnerability CVE ID : CVE-2021-1662	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1662	O-MIC-WIND-210121/719
Exposure of Sensitive Information to an Unauthorized Actor	12-Jan-21	2.1	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-1670, CVE-2021-1672. CVE ID : CVE-2021-1663	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1663	O-MIC-WIND-210121/720
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1663	O-MIC-WIND-210121/721

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1666, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1664	osoft.com/en-US/security-guidance/advisory/CVE-2021-1664	
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1664, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1666	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1666	O-MIC-WIND-210121/722

windows_server_2019

Incorrect Authorization	12-Jan-21	2.1	Windows Bluetooth Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-1683, CVE-2021-1684. CVE ID : CVE-2021-1638	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1638	O-MIC-WIND-210121/723
Improper Privilege Management	12-Jan-21	4.6	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1685. CVE ID : CVE-2021-1642	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1642	O-MIC-WIND-210121/724
Not Available	12-Jan-21	4.3	Windows Docker Information Disclosure Vulnerability	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210121/725

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1645	US/security-guidance/advisory/CVE-2021-1645	
Improper Privilege Management	12-Jan-21	7.2	Windows WLAN Service Elevation of Privilege Vulnerability CVE ID : CVE-2021-1646	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1646	O-MIC-WIND-210121/726
Not Available	12-Jan-21	7.2	Microsoft Defender Remote Code Execution Vulnerability CVE ID : CVE-2021-1647	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1647	O-MIC-WIND-210121/727
Improper Privilege Management	12-Jan-21	7.2	Microsoft splwow64 Elevation of Privilege Vulnerability CVE ID : CVE-2021-1648	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1648	O-MIC-WIND-210121/728
Improper Privilege Management	12-Jan-21	7.2	Active Template Library Elevation of Privilege Vulnerability CVE ID : CVE-2021-1649	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1649	O-MIC-WIND-210121/729
Improper Privilege Management	12-Jan-21	7.2	Windows Runtime C++ Template Library Elevation of Privilege Vulnerability	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1649	O-MIC-WIND-210121/730

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1650	n-US/security-guidance/advisory/CVE-2021-1650	
Improper Privilege Management	12-Jan-21	9	Windows LUAFV Elevation of Privilege Vulnerability CVE ID : CVE-2021-1706	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1706	O-MIC-WIND-210121/731
Not Available	12-Jan-21	6.8	Microsoft Windows Media Foundation Remote Code Execution Vulnerability CVE ID : CVE-2021-1710	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1710	O-MIC-WIND-210121/732
Improper Privilege Management	12-Jan-21	7.2	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1680. CVE ID : CVE-2021-1651	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1651	O-MIC-WIND-210121/733
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1653, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1652	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1652	O-MIC-WIND-210121/734
Improper	12-Jan-21	7.2	Windows CSC Service	https://port	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1654, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1653	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1653	210121/735
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1655, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1654	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1654	O-MIC-WIND-210121/736
Improper Privilege Management	12-Jan-21	7.2	Windows CSC Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1652, CVE-2021-1653, CVE-2021-1654, CVE-2021-1659, CVE-2021-1688, CVE-2021-1693. CVE ID : CVE-2021-1655	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1655	O-MIC-WIND-210121/737
Not Available	12-Jan-21	2.1	TPM Device Driver Information Disclosure Vulnerability CVE ID : CVE-2021-1656	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1656	O-MIC-WIND-210121/738
Improper Privilege Management	12-Jan-21	7.2	Windows Fax Compose Form Remote Code Execution Vulnerability CVE ID : CVE-2021-1657	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210121/739

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2021-1657	
Improper Privilege Management	12-Jan-21	4.6	Windows Event Tracing Elevation of Privilege Vulnerability CVE ID : CVE-2021-1662	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1662	O-MIC-WIND-210121/740
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1666, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1664	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1664	O-MIC-WIND-210121/741
Not Available	12-Jan-21	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-1658, CVE-2021-1660, CVE-2021-1664, CVE-2021-1667, CVE-2021-1671, CVE-2021-1673, CVE-2021-1700, CVE-2021-1701. CVE ID : CVE-2021-1666	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1666	O-MIC-WIND-210121/742

Mikrotik

routeros

Improper Neutralization of Input During Web Page	04-Jan-21	4.3	In MikroTik RouterOS through 2021-01-04, the hotspot login page is vulnerable to reflected XSS via the target parameter.	N/A	O-MIK-ROUT-210121/743
--	-----------	-----	--	-----	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			CVE ID : CVE-2021-3014		
nutanix					
ahv					
Allocation of Resources Without Limits or Throttling	08-Jan-21	4.6	NVIDIA Virtual GPU Manager NVIDIA vGPU manager contains a vulnerability in the vGPU plugin in which it allows guests to allocate some resources for which the guest is not authorized, which may lead to integrity and confidentiality loss, denial of service, or information disclosure. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1057	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-NUT-AHV-210121/744
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input data size is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1058	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-NUT-AHV-210121/745
Integer Overflow or Wraparound	08-Jan-21	4.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input index is not validated, which may lead to integer overflow, which in turn may cause tampering of data, information disclosure, or	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-NUT-AHV-210121/746

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1059		
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input index is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1060	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-NUT-AHV-210121/747
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-21	3.3	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which a race condition may cause the vGPU plugin to continue using a previously validated resource that has since changed, which may lead to denial of service or information disclosure. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1061	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-NUT-AHV-210121/748
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input data length is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-NUT-AHV-210121/749

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2021-1062							
Out-of-bounds Read	08-Jan-21	4.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input offset is not validated, which may lead to a buffer overread, which in turn may cause tampering of data, information disclosure, or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1063	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-NUT-AHV-210121/750					
NULL Pointer Dereference	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which it obtains a value from an untrusted source, converts this value to a pointer, and dereferences the resulting pointer, which may lead to information disclosure or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1064	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-NUT-AHV-210121/751					
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which input data is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1065	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-NUT-AHV-210121/752					
Uncontrolled	08-Jan-21	2.1	NVIDIA vGPU manager	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-NUT-AHV-210121/753					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			contains a vulnerability in the vGPU plugin, in which input data is not validated, which may lead to unexpected consumption of resources, which in turn may lead to denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1066	ia.custhelp.com/app/answers/detail/a_id/5142	210121/753

Paloaltonetworks

pan-os

Exposure of Sensitive Information to an Unauthorized Actor	13-Jan-21	3.3	Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions	https://security.paloaltonetworks.com/CVE-2021-3031	O-PAL-PAN--210121/754
--	-----------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than PAN-OS 9.1.5. CVE ID : CVE-2021-3031		
Insertion of Sensitive Information into Log File	13-Jan-21	2.1	An information exposure through log file vulnerability exists in Palo Alto Networks PAN-OS software where configuration secrets for the “http”, “email”, and “snmptrap” v3 log forwarding server profiles can be logged to the logrcvr.log system log. Logged information may include up to 1024 bytes of the configuration including the username and password in an encrypted form and private keys used in any certificate profiles set for log forwarding server profiles. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.4; PAN-OS 10.0 versions earlier than PAN-OS 10.0.1. CVE ID : CVE-2021-3032	https://security.paloaltonetworks.com/CVE-2021-3032	O-PAL-PAN--210121/755

Redhat

enterprise_linux_kernel-based_virtual_machine

Allocation of Resources Without Limits or Throttling	08-Jan-21	4.6	NVIDIA Virtual GPU Manager NVIDIA vGPU manager contains a vulnerability in the vGPU plugin in which it allows guests to allocate some resources for which the guest is not authorized, which may lead to integrity	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-RED-ENTE-210121/756
--	-----------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and confidentiality loss, denial of service, or information disclosure. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1057		
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input data size is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1058	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-RED-ENTE-210121/757
Integer Overflow or Wraparound	08-Jan-21	4.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input index is not validated, which may lead to integer overflow, which in turn may cause tampering of data, information disclosure, or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1059	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-RED-ENTE-210121/758
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input index is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-RED-ENTE-210121/759

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1060		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-21	3.3	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which a race condition may cause the vGPU plugin to continue using a previously validated resource that has since changed, which may lead to denial of service or information disclosure. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1061	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-RED-ENTE-210121/760
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input data length is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1062	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-RED-ENTE-210121/761
Out-of-bounds Read	08-Jan-21	4.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input offset is not validated, which may lead to a buffer overread, which in turn may cause tampering of data, information disclosure, or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-RED-ENTE-210121/762

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1063		
NULL Pointer Dereference	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which it obtains a value from an untrusted source, converts this value to a pointer, and dereferences the resulting pointer, which may lead to information disclosure or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1064	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-RED-ENTE-210121/763
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which input data is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1065	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-RED-ENTE-210121/764
Uncontrolled Resource Consumption	08-Jan-21	2.1	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which input data is not validated, which may lead to unexpected consumption of resources, which in turn may lead to denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1066	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-RED-ENTE-210121/765

Vmware

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vsphere					
Allocation of Resources Without Limits or Throttling	08-Jan-21	4.6	NVIDIA Virtual GPU Manager NVIDIA vGPU manager contains a vulnerability in the vGPU plugin in which it allows guests to allocate some resources for which the guest is not authorized, which may lead to integrity and confidentiality loss, denial of service, or information disclosure. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1057	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-VMW-VSPH-210121/766
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input data size is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1058	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-VMW-VSPH-210121/767
Integer Overflow or Wraparound	08-Jan-21	4.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input index is not validated, which may lead to integer overflow, which in turn may cause tampering of data, information disclosure, or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-VMW-VSPH-210121/768

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2021-1059							
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input index is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1060	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-VMW-VSPH-210121/769					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-21	3.3	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which a race condition may cause the vGPU plugin to continue using a previously validated resource that has since changed, which may lead to denial of service or information disclosure. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1061	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-VMW-VSPH-210121/770					
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input data length is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1062	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-VMW-VSPH-210121/771					
Out-of-bounds Read	08-Jan-21	4.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an	https://nvidia.custhelp.com/app/ans	O-VMW-VSPH-210121/772					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input offset is not validated, which may lead to a buffer overread, which in turn may cause tampering of data, information disclosure, or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1063	wers/detail/a_id/5142	
NULL Pointer Dereference	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which it obtains a value from an untrusted source, converts this value to a pointer, and dereferences the resulting pointer, which may lead to information disclosure or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1064	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-VMW-VSPH-210121/773
Improper Input Validation	08-Jan-21	3.6	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which input data is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1065	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-VMW-VSPH-210121/774
Uncontrolled Resource Consumption	08-Jan-21	2.1	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which input data is not validated, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5142	O-VMW-VSPH-210121/775

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected consumption of resources, which in turn may lead to denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3). CVE ID : CVE-2021-1066		

Hardware

Cisco

isr_4431

Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1223	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	H-CIS-ISR_-210121/776
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-	H-CIS-ISR_-210121/777

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	MmzZrtes	
Always-Incorrect Control Flow Implementation	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network.</p> <p>CVE ID : CVE-2021-1236</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-ISR_-210121/778
isr_4461					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1223</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	H-CIS-ISR_-210121/779
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-ISR_-210121/780

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224		
Always- Incorrect Control Flow Implementat ion	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network. CVE ID : CVE-2021-1236	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-ISR_-210121/781
rv110w					
Improper Neutralizatio n of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	H-CIS-RV11-210121/782

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1146</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	H-CIS-RV11-210121/783

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1147</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	H-CIS-RV11-210121/784

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1148		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1149	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	H-CIS-RV11-210121/785
Improper Neutralization of Special	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/s	H-CIS-RV11-210121/786

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1150	er/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV11-210121/787

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1151</p>		
<p>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</p>	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	H-CIS-RV11-210121/788

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1152							
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1153	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV11-210121/789					
Improper	13-Jan-21	3.5	Multiple vulnerabilities in	https://tools	H-CIS-RV11-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1154</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	210121/790
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	H-CIS-RV11-210121/791

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1155</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	H-CIS-RV11-210121/792

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1156							
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1157	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV11-210121/793					
Improper	13-Jan-21	3.5	Multiple vulnerabilities in	https://tools	H-CIS-RV11-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1158</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	210121/794
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/795

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1159</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/796

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1160</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/797

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1161</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/798

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1162</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/799

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1163</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/800

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1164		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/801

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1165		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1166</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/802
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	H-CIS-RV11-210121/803

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1167</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV11-210121/804

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1168</p>	overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/805

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1169</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/806

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1170</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/807

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1171</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/808

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1172		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/809

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1173</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/810

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1174		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/811

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1175		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1176</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/812
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	H-CIS-RV11-210121/813

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1177</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV11-210121/814

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1178</p>	overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/815

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1179</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/816

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1180</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/817

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1181</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/818

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1182		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/819

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1183</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/820

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1184		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/821

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1185		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1186</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/822
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	H-CIS-RV11-210121/823

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1187</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV11-210121/824

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1188</p>	overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/825

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1189</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/826

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1190</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/827

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1191</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/828

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1192</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/829

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1193</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/830

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1194		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/831

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1195		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1196</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/832
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	H-CIS-RV11-210121/833

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1197</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/834

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1198</p>	overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/835

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1199</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/836

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1200</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/837

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1201</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/838

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1202		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/839

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1203</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/840

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1204		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/841

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1205		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1206</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/842
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	H-CIS-RV11-210121/843

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1207</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/844

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1208</p>	overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/845

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1209</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/846

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1210</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/847

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1211</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/848

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1212		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/849

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1213</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV11-210121/850

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1214		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/851

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1215		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1216</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV11-210121/852
rv130w					
Improper Neutralization	13-Jan-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	H-CIS-RV13-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1146	security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	210121/853
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	H-CIS-RV13-210121/854

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1147</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	H-CIS-RV13-210121/855

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1148</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	H-CIS-RV13-210121/856

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			<p>credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1149</p>							
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1150</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	H-CIS-RV13-210121/857					
Improper Neutralization	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	H-CIS-RV13-210121/858					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1151	security/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input	https://tools.cisco.com/security/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV13-210121/859

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1152		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV13-210121/860

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1153							
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1154	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV13-210121/861					
Improper Neutralization	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	H-CIS-RV13-210121/862					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1155	security/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input	https://tools.cisco.com/security/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV13-210121/863

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1156</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	H-CIS-RV13-210121/864

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1157							
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1158	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV13-210121/865					
Out-of-bounds	13-Jan-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	H-CIS-RV13-210121/866					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			<p>interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1159</p>	<p>ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/867

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1160</p>	sco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/868

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1161</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/869

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1162</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/870

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1163</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/871

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1164</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/872

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1165</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/873

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1166</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/874

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			vulnerabilities. CVE ID : CVE-2021-1167							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1168	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/875					
Out-of-bounds	13-Jan-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	H-CIS-RV13-210121/876					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			<p>interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1169</p>	<p>ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/877

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1170</p>	sco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/878

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1171</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/879

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1172</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/880

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1173</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/881

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1174</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/882

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1175</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/883

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1176</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/884

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			vulnerabilities. CVE ID : CVE-2021-1177							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1178	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/885					
Out-of-bounds	13-Jan-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	H-CIS-RV13-210121/886					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			<p>interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1179</p>	<p>ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/887

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1180</p>	sco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/888

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1181</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/889

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1182</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/890

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1183</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/891

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1184</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/892

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1185</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/893

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1186</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/894

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			vulnerabilities. CVE ID : CVE-2021-1187							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1188	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/895					
Out-of-bounds	13-Jan-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	H-CIS-RV13-210121/896					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			<p>interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1189</p>	<p>ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/897

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1190</p>	sco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/898

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1191</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/899

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1192</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/900

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1193</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/901

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1194</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/902

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1195</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/903

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1196</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/904

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			vulnerabilities. CVE ID : CVE-2021-1197							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1198	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/905					
Out-of-bounds	13-Jan-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	H-CIS-RV13-210121/906					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			<p>interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1199</p>	<p>ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/907

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1200</p>	sco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/908

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1201</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/909

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1202</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/910

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1203</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/911

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1204</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/912

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1205</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/913

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1206</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/914

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			vulnerabilities. CVE ID : CVE-2021-1207							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1208	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/915					
Out-of-bounds	13-Jan-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	H-CIS-RV13-210121/916					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			<p>interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1209</p>	<p>ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/917

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1210</p>	sco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/918

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1211</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/919

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1212</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/920

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1213</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/921

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1214</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/922

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1215</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/923

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1216</p>		
rv215w					
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/924

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			that address these vulnerabilities. CVE ID : CVE-2021-1179							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1180	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/925					
Out-of-	13-Jan-21	9	Multiple vulnerabilities in	https://tools	H-CIS-RV21-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1181</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/926
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/927

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1182</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/928

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1183</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/929

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1190</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/930

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1191</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/931

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1200</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/932

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1201</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/933

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1202</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/934

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			that address these vulnerabilities. CVE ID : CVE-2021-1203							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1204	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/935					
Out-of-	13-Jan-21	9	Multiple vulnerabilities in	https://tools	H-CIS-RV21-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1205</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/936
isr_4451-x					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an	https://tools.cisco.com/security/center/content/	H-CIS-ISR_-210121/937

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1223</p>	<p>CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2</p>	
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes</p>	H-CIS-ISR_-210121/938

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious payload. CVE ID : CVE-2021-1224		
Always- Incorrect Control Flow Implementat ion	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network. CVE ID : CVE-2021-1236	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-ISR_-210121/939
meraki_mx64					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-MERA-210121/940

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224		

meraki_mx64w

Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-MERA-210121/941
-------------------------------	-----------	---	---	---	-----------------------

meraki_mx67

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-MERA-210121/942

meraki_mx67c

Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-MERA-210121/943
-------------------------------	-----------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			<p>within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>							
meraki_mx67w										
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes</p>	H-CIS-MERA-210121/944					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
meraki_mx68					
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-MERA-210121/945
meraki_mx68cw					
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-MERA-210121/946

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>		

meraki_mx68w

Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes</p>	H-CIS-MERA-210121/947
-------------------------------	-----------	---	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1224		
meraki_mx100					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-MERA-210121/948
meraki_mx84					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-MERA-210121/949

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>		

meraki_mx250

Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes</p>	H-CIS-MERA-210121/950
-------------------------------	-----------	---	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224		
meraki_mx450					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-MERA-210121/951
rv130					
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	H-CIS-RV13-210121/952

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1179	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/953

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1180</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV13-210121/954

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1181</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/955

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1182		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV13-210121/956

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1183</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/957

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1190</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/958

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1191		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1200	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/959

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1201</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/960
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	H-CIS-RV13-210121/961

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1202</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	H-CIS-RV13-210121/962

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1203	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/963

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1204</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV13-210121/964

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1205</p>		

isr_4321

Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2</p>	H-CIS-ISR-210121/965
-------------------------------	-----------	---	--	--	----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1223		
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-ISR_-210121/966
Always-Incorrect Control Flow Implementation	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-ISR_-210121/967

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network.</p> <p>CVE ID : CVE-2021-1236</p>		
isr_4351					
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1223</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	H-CIS-ISR_-210121/968
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-ISR_-210121/969

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>		
Always- Incorrect Control Flow Implementat ion	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network.</p> <p>CVE ID : CVE-2021-1236</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-ISR_- 210121/970
csr_1000v					
Improper	13-Jan-21	5	Multiple Cisco products are	https://tools	H-CIS-CSR_-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			<p>affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1223</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	210121/971
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes</p>	H-CIS-CSR_-210121/972

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224		
Always- Incorrect Control Flow Implementat ion	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network. CVE ID : CVE-2021-1236	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-CSR_-210121/973
isr_4221					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	H-CIS-ISR_-210121/974

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1223		
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-ISR_-210121/975
Always-Incorrect Control Flow Implementation	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-ISR_-210121/976

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network.</p> <p>CVE ID : CVE-2021-1236</p>	sco-sa-snort-app-bypass-cSBYCATq	
isr_4331					
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1223</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	H-CIS-ISR_-210121/977
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO)</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tcpfastopen-67DEwMe2	H-CIS-ISR_-210121/978

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	er/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	
Always-Incorrect Control Flow Implementation	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-ISR_-210121/979

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			policies and deliver a malicious payload to the protected network. CVE ID : CVE-2021-1236		
isa_3000					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1223	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	H-CIS-ISA_-210121/980
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-ISA_-210121/981

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224		
Always- Incorrect Control Flow Implementat ion	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network. CVE ID : CVE-2021-1236	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-ISA_-210121/982
rv110w_wireless-n_vpn_firewall					
Out-of- bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-RV11-210121/983

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1217</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
rv130_vpn_router					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-	H-CIS-RV13-210121/984

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1146</p>	inject-LBdQ2KRN	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	H-CIS-RV13-210121/985

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1147</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	H-CIS-RV13-210121/986

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1148</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1149</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	H-CIS-RV13-210121/987

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1150	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	H-CIS-RV13-210121/988
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-	H-CIS-RV13-210121/989

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1151</p>	LPTQ3EQC	
<p>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</p>	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	H-CIS-RV13-210121/990

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1152</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	H-CIS-RV13-210121/991

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			device. CVE ID : CVE-2021-1153							
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1154	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV13-210121/992					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-	H-CIS-RV13-210121/993					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1155</p>	LPTQ3EQC	
<p>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</p>	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	H-CIS-RV13-210121/994

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1156</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	H-CIS-RV13-210121/995

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. CVE ID : CVE-2021-1157		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1158	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV13-210121/996
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	H-CIS-RV13-210121/997

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1159	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/998

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1160</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV13-210121/999

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1161</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1000

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1162</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV13-210121/1001

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1163</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1002

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1164</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1003

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1165		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1166	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/1004

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1167</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1005
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	H-CIS-RV13-210121/1006

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1168</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	H-CIS-RV13-210121/1007

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1169	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/1008

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1170</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV13-210121/1009

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1171</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1010

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1172		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV13-210121/1011

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1173</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1012

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1174</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1013

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1175		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1176	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/1014

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1177</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1015
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	H-CIS-RV13-210121/1016

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1178</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	H-CIS-RV13-210121/1017

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1184	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/1018

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1185</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV13-210121/1019

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1186</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1020

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1187</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV13-210121/1021

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1188</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1022

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1189</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1023

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1192		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1193	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/1024

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1194</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1025
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	H-CIS-RV13-210121/1026

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1195</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	H-CIS-RV13-210121/1027

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1196	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/1028

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1197</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV13-210121/1029

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1198</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1030

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1199</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV13-210121/1031

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1206</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1032

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1207</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1033

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			released software updates that address these vulnerabilities. CVE ID : CVE-2021-1208		
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1209	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/1034

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1210</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1035
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130,</p>	<p>https://tools.cisco.com/security/center/content/</p>	H-CIS-RV13-210121/1036

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1211</p>	CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-</p>	H-CIS-RV13-210121/1037

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1212	WUnUgv4U	
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	H-CIS-RV13-210121/1038

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1213</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV13-210121/1039

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1214</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1040

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1215</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV13-210121/1041

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1216</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1042

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1217</p>		

rv130w_wireless-n_multifunction_vpn_router

Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV13-210121/1043
---------------------	-----------	---	---	--	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1217		
rv215w_wireless-n_vpn_router					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1146	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	H-CIS-RV21-210121/1044
Improper	13-Jan-21	9	Multiple vulnerabilities in	https://tools	H-CIS-RV21-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1147</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	210121/1045
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-	H-CIS-RV21-210121/1046

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1148</p>	LBdQ2KRN	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN</p>	H-CIS-RV21-210121/1047

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1149		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-LBdQ2KRN	H-CIS-RV21-210121/1048

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1150		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1151	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV21-210121/1049
Improper Neutralization of Input	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	H-CIS-RV21-210121/1050

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1152	er/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV21-210121/1051

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1153</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	H-CIS-RV21-210121/1052

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1154		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1155	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV21-210121/1053
Improper Neutralization of Input	13-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	H-CIS-RV21-210121/1054

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			<p>Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1156</p>	er/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC	H-CIS-RV21-210121/1055

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1157</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jan-21	3.5	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-LPTQ3EQC</p>	H-CIS-RV21-210121/1056

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1158</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1057

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			that address these vulnerabilities. CVE ID : CVE-2021-1159							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1160	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/1058					
Out-of-	13-Jan-21	9	Multiple vulnerabilities in	https://tools	H-CIS-RV21-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1161</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/1059
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurit</p>	H-CIS-RV21-210121/1060

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1162</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/1061

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1163</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1062

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1164</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1063

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1165</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1064

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1166</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/1065

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1167</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/1066

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1168</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1067

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			that address these vulnerabilities. CVE ID : CVE-2021-1169							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1170	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/1068					
Out-of-	13-Jan-21	9	Multiple vulnerabilities in	https://tools	H-CIS-RV21-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1171</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/1069
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/1070

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1172</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/1071

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1173</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1072

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1174</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1073

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1175</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1074

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1176</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/1075

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1177</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/1076

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1178</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1077

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			that address these vulnerabilities. CVE ID : CVE-2021-1184							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1185	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/1078					
Out-of-	13-Jan-21	9	Multiple vulnerabilities in	https://tools	H-CIS-RV21-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1186</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/1079
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/1080

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1187</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/1081

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1188</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1082

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1189</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1083

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1192</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1084

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1193</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/1085

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1194</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/1086

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1195</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1087

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			that address these vulnerabilities. CVE ID : CVE-2021-1196							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1197	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/1088					
Out-of-	13-Jan-21	9	Multiple vulnerabilities in	https://tools	H-CIS-RV21-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1198</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/1089
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/1090

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1199</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/1091

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1206</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1092

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1207</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1093

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1208</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1094

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1209</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload,</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/1095

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1210</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/1096

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1211</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1097

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			that address these vulnerabilities. CVE ID : CVE-2021-1212							
Out-of-bounds Write	13-Jan-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities. CVE ID : CVE-2021-1213	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/1098					
Out-of-	13-Jan-21	9	Multiple vulnerabilities in	https://tools	H-CIS-RV21-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			<p>the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1214</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U	210121/1099
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U</p>	H-CIS-RV21-210121/1100

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1215</p>	yAdvisory/cisco-sa-rv-overflow-WUnUgy4U	
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U	H-CIS-RV21-210121/1101

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1216</p>		
Out-of-bounds Write	13-Jan-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgy4U</p>	H-CIS-RV21-210121/1102

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.</p> <p>CVE ID : CVE-2021-1217</p>		

isr_1100-4p

Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2</p>	H-CIS-ISR-210121/1103
-------------------------------	-----------	---	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1223		
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-ISR_-210121/1104
Always-Incorrect Control Flow Implementation	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-ISR_-210121/1105

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network. CVE ID : CVE-2021-1236		
isr_1100-8p					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1223	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	H-CIS-ISR_-210121/1106
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-	H-CIS-ISR_-210121/1107

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	tfo-bypass-MmzZrtes	
Always-Incorrect Control Flow Implementation	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network.</p> <p>CVE ID : CVE-2021-1236</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-ISR_-210121/1108

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
isr_1101-4p					
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1223</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	H-CIS-ISR_-210121/1109
Improper Privilege Management	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-ISR_-210121/1110

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224		
Always-Incorrect Control Flow Implementation	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network. CVE ID : CVE-2021-1236	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-ISR_-210121/1111

isr_1109-2p

Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	H-CIS-ISR_-210121/1112
-------------------------------	-----------	---	--	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1223		
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1224	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-ISR_-210121/1113
Always-Incorrect Control Flow Implementat	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could	https://tools.cisco.com/security/center/content/	H-CIS-ISR_-210121/1114

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion			allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network. CVE ID : CVE-2021-1236	CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	
isr_1109-4p					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1223	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	H-CIS-ISR_-210121/1115
Improper	13-Jan-21	5	Multiple Cisco products are	https://tools	H-CIS-ISR_-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			<p>affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	210121/1116
Always-Incorrect Control Flow Implementation	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq</p>	H-CIS-ISR_-210121/1117

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network. CVE ID : CVE-2021-1236		
isr_1111x-8p					
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload. CVE ID : CVE-2021-1223	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2	H-CIS-ISR_-210121/1118
Improper Privilege Management	13-Jan-21	5	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes	H-CIS-ISR_-210121/1119

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.</p> <p>CVE ID : CVE-2021-1224</p>		
Always-Incorrect Control Flow Implementation	13-Jan-21	5	<p>Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network.</p> <p>CVE ID : CVE-2021-1236</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq	H-CIS-ISR-210121/1120
mercusys					
mercury_x18g					
Improper Limitation of	07-Jan-21	5	MERCUSYS Mercury X18G 1.0.5 devices allow Directory	https://www.mercuryco	H-MER-MERC-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			Traversal via ../ in conjunction with a loginLess or login.htm URI (for authentication bypass) to the web server, as demonstrated by the /loginLess/../../etc/passwd URI. CVE ID : CVE-2021-23241	m.com.cn/product-521-1.html, https://www.mercusys.com/en/	210121/1121
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jan-21	5	MERCUSYS Mercury X18G 1.0.5 devices allow Directory Traversal via ../ to the UPnP server, as demonstrated by the ../../conf/template/uhttpd.json URI. CVE ID : CVE-2021-23242	https://www.mercurycom.com.cn/product-521-1.html, https://www.mercusys.com/en/	H-MER-MERC-210121/1122

Paloaltonetworks

pa-200

Exposure of Sensitive Information to an Unauthorized Actor	13-Jan-21	3.3	Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security	https://security.paloaltonetworks.com/CVE-2021-3031	H-PAL-PA-2-210121/1123
--	-----------	-----	---	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5. CVE ID : CVE-2021-3031		

pa-2020

Exposure of Sensitive Information to an Unauthorized Actor	13-Jan-21	3.3	Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5. CVE ID : CVE-2021-3031	https://security.paloaltonetworks.com/CVE-2021-3031	H-PAL-PA-2-210121/1124
--	-----------	-----	---	---	------------------------

pa-2050

Exposure of	13-Jan-21	3.3	Padding bytes in Ethernet	https://secu	H-PAL-PA-2-
-------------	-----------	-----	---------------------------	---	-------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information to an Unauthorized Actor			packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5. CVE ID : CVE-2021-3031	rity.paloalto networks.com/CVE-2021-3031	210121/1125

pa-220

Exposure of Sensitive Information to an Unauthorized Actor	13-Jan-21	3.3	Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An	https://security.paloalto networks.com/CVE-2021-3031	H-PAL-PA-2-210121/1126
--	-----------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5.</p> <p>CVE ID : CVE-2021-3031</p>		

pa-3020

Exposure of Sensitive Information to an Unauthorized Actor	13-Jan-21	3.3	<p>Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-</p>	<p>https://security.paloaltonetworks.com/CVE-2021-3031</p>	H-PAL-PA-3-210121/1127
--	-----------	-----	--	--	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5. CVE ID : CVE-2021-3031		
pa-3050					
Exposure of Sensitive Information to an Unauthorized Actor	13-Jan-21	3.3	Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5. CVE ID : CVE-2021-3031	https://security.paloaltonetworks.com/CVE-2021-3031	H-PAL-PA-3-210121/1128
pa-3060					
Exposure of Sensitive Information to an	13-Jan-21	3.3	Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-	https://security.paloaltonetworks.com/CVE-	H-PAL-PA-3-210121/1129

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5. CVE ID : CVE-2021-3031	2021-3031	

pa-3220

Exposure of Sensitive Information to an Unauthorized Actor	13-Jan-21	3.3	Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect	https://security.paloaltonetworks.com/CVE-2021-3031	H-PAL-PA-3-210121/1130
--	-----------	-----	---	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5. CVE ID : CVE-2021-3031		

pa-3250

Exposure of Sensitive Information to an Unauthorized Actor	13-Jan-21	3.3	Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions	https://security.paloaltonetworks.com/CVE-2021-3031	H-PAL-PA-3-210121/1131
--	-----------	-----	---	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than PAN-OS 9.1.5. CVE ID : CVE-2021-3031		
pa-3260					
Exposure of Sensitive Information to an Unauthorized Actor	13-Jan-21	3.3	Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5. CVE ID : CVE-2021-3031	https://security.paloaltonetworks.com/CVE-2021-3031	H-PAL-PA-3-210121/1132
pa-500					
Exposure of Sensitive Information to an Unauthorized Actor	13-Jan-21	3.3	Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the	https://security.paloaltonetworks.com/CVE-2021-3031	H-PAL-PA-5-210121/1133

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5.</p> <p>CVE ID : CVE-2021-3031</p>		

pa-5200

Exposure of Sensitive Information to an Unauthorized Actor	13-Jan-21	3.3	<p>Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also</p>	<p>https://security.paloaltonetworks.com/CVE-2021-3031</p>	H-PAL-PA-5-210121/1134
--	-----------	-----	---	--	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5.</p> <p>CVE ID : CVE-2021-3031</p>		
pa-800					
Exposure of Sensitive Information to an Unauthorized Actor	13-Jan-21	3.3	<p>Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5.</p> <p>CVE ID : CVE-2021-3031</p>	<p>https://security.paloaltonetworks.com/CVE-2021-3031</p>	H-PAL-PA-8-210121/1135

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Samsung					
exynos					
Out-of-bounds Write	05-Jan-21	7.1	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), Q(10.0), and R(11.0) (Exynos chipsets) software. The Mali GPU driver allows out-of-bounds access and a device reset. The Samsung ID is SVE-2020-19174 (January 2021). CVE ID : CVE-2021-22495	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-EXYN-210121/1136
galaxy_note_20					
Not Available	05-Jan-21	4.3	An issue was discovered in the fingerprint scanner on Samsung Note20 mobile devices with Q(10.0) software. When a screen protector is used, the required image compensation is not present. Consequently, inversion can occur during fingerprint enrollment, and a high False Recognition Rate (FRR) can occur. The Samsung ID is SVE-2020-19216 (January 2021). CVE ID : CVE-2021-22494	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-GALA-210121/1137

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