



CVE-2021-1180

Published on: 01/13/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:55 PM UTC

CVE-2021-1180 - advisory for cisco-sa-rv-overflow-WUnUgv4U

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Rv110w](#) from [Cisco](#) contain the following vulnerability:

Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in

the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these 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-2021-1180 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

Affected Vendor/Software: [Cisco](#) - **Cisco Small Business RV Series Router Firmware** version **n/a**

CVSS3 Score: **7.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Remote Command Execution and Denial of Service Vulnerabilities	Vendor Advisory tools.cisco.com text/html	CISCO 20210113 Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Management Interface Remote Command Execution and Denial of Service Vulnerabilities

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Cisco	Rv110w	-	All	All	All
Hardware 	Cisco	Rv110w	-	All	All	All
Hardware 	Cisco	Rv110w	-	All	All	All
Operating System	Cisco	Rv110w Firmware	1.0.3.44	All	All	All
Operating System	Cisco	Rv110w Firmware	1.0.3.44	All	All	All
Hardware 	Cisco	Rv130	-	All	All	All
Hardware 	Cisco	Rv130	-	All	All	All
Hardware 	Cisco	Rv130	-	All	All	All
Hardware 	Cisco	Rv130w	-	All	All	All
Hardware 	Cisco	Rv130w	-	All	All	All
Hardware 	Cisco	Rv130w	-	All	All	All
Operating System	Cisco	Rv130w Firmware	1.0.3.44	All	All	All
Operating System	Cisco	Rv130w Firmware	1.0.3.44	All	All	All
Operating System	Cisco	Rv130 Firmware	1.0.3.44	All	All	All
Operating System	Cisco	Rv130 Firmware	1.0.3.44	All	All	All

Hardware 	Cisco	Rv215w	-	All	All	All
Hardware 	Cisco	Rv215w	-	All	All	All
Hardware 	Cisco	Rv215w	-	All	All	All
Operating System	Cisco	Rv215w Firmware	1.0.3.44	All	All	All
Operating System	Cisco	Rv215w Firmware	1.0.3.44	All	All	All
cpe:2.3:h:cisco:rv110w:-:*:*:*:*:*:						
cpe:2.3:h:cisco:rv110w:-:*:*:*:*:*:						
cpe:2.3:h:cisco:rv110w:-:*:*:*:*:*:						
cpe:2.3:o:cisco:rv110w_firmware:1.0.3.44:*:*:*:*:*:						
cpe:2.3:o:cisco:rv110w_firmware:1.0.3.44:*:*:*:*:*:						
cpe:2.3:h:cisco:rv130:-:*:*:*:*:*:						
cpe:2.3:h:cisco:rv130:-:*:*:*:*:*:						
cpe:2.3:h:cisco:rv130:-:*:*:*:*:*:						
cpe:2.3:h:cisco:rv130w:-:*:*:*:*:*:						
cpe:2.3:h:cisco:rv130w:-:*:*:*:*:*:						
cpe:2.3:h:cisco:rv130w:-:*:*:*:*:*:						
cpe:2.3:o:cisco:rv130w_firmware:1.0.3.44:*:*:*:*:*:						
cpe:2.3:o:cisco:rv130w_firmware:1.0.3.44:*:*:*:*:*:						
cpe:2.3:o:cisco:rv130_firmware:1.0.3.44:*:*:*:*:*:						
cpe:2.3:o:cisco:rv130_firmware:1.0.3.44:*:*:*:*:*:						
cpe:2.3:h:cisco:rv215w:-:*:*:*:*:*:						
cpe:2.3:h:cisco:rv215w:-:*:*:*:*:*:						
cpe:2.3:h:cisco:rv215w:-:*:*:*:*:*:						
cpe:2.3:o:cisco:rv215w_firmware:1.0.3.44:*:*:*:*:*:						
cpe:2.3:o:cisco:rv215w_firmware:1.0.3.44:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)