



CVE-2022-20893

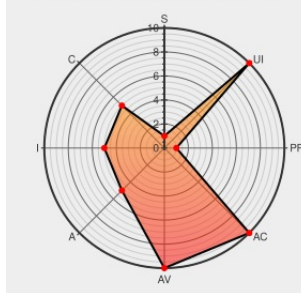
Published on: Not Yet Published

Last Modified on: 07/26/2022 02:39:00 PM UTC

CVE-2022-20893 - advisory for cisco-sa-sb-rv-rce-overflow-ygHByAK

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

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



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 on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insufficient validation of user fields within incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these 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-2022-20893 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities that are described in this advisory.

Affected Vendor/Software: [Cisco](#) **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

CVE References

Description	Tags	Link
-------------	------	------

 CISCO 20220720 Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers
 Remote Command Execution and Denial of Service Vulnerabilities

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Rv110w	-	All	All	All
Operating System	Cisco	Rv110w Firmware	1.3.1.7	All	All	All
Hardware	Cisco	Rv130	-	All	All	All
Hardware	Cisco	Rv130w	-	All	All	All
Operating System	Cisco	Rv130w Firmware	1.3.1.7	All	All	All
Operating System	Cisco	Rv130 Firmware	1.3.1.7	All	All	All
Hardware	Cisco	Rv215w	-	All	All	All
Operating System	Cisco	Rv215w Firmware	1.3.1.7	All	All	All
cpe:2.3:h:cisco:rv110w:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:rv110w_firmware:1.3.1.7:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:cisco:rv130:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:cisco:rv130w:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:rv130w_firmware:1.3.1.7:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:rv130_firmware:1.3.1.7:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:cisco:rv215w:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:rv215w_firmware:1.3.1.7:~::~~::~~::~~::~~::~~::~~:::						

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-20893 : Multiple vulnerabilities in the web-based management interface of Cisco Small	2022-07-22

Business RV110W, RV1... twitter.com/i/web/status/1...		03:33:04
 /r/netcve	CVE-2022-20893	2022-07-22 04:38:44
← Previous ID		Next ID →

© [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](#)