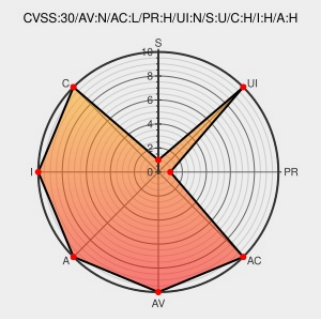
CVE-2020-3290

Published on: 06/17/2020 12:00:00 AM UTC

Last Modified on: 08/06/2021 06:44:00 PM UTC

CVE-2020-3290 - advisory for cisco-sa-rv-routers-stack-vUxHmnNz

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Rv016 from Cisco contain the following vulnerability:

Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system.

CVE-2020-3290 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH severity.

The Cisco Product Security Incident Response Team (PSIRT) is aware that proof-of-concept exploit code is available for the vulnerabilities that are 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 RV Series Routers Stack Overflow Arbitrary Code Execution Vulnerabilities	Vendor Advisory tools.cisco.com text/html	CISCO 20200617 Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution Vulnerabilities

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Rv016	-	All	All	All
Hardware	Cisco	Rv016	-	All	All	All
Operating System	Cisco	Rv016 Firmware	All	All	All	All
Hardware	Cisco	Rv042	-	All	All	All
Hardware	Cisco	Rv042	-	All	All	All
Hardware	Cisco	Rv042g	-	All	All	All
Hardware	Cisco	Rv042g	-	All	All	All
Operating System	Cisco	Rv042g Firmware	All	All	All	All
Operating System	Cisco	Rv042 Firmware	All	All	All	All
Hardware	Cisco	Rv082	-	All	All	All
Hardware	Cisco	Rv082	-	All	All	All
Operating System	Cisco	Rv082 Firmware	All	All	All	All
Hardware	Cisco	Rv320	-	All	All	All
Hardware	Cisco	Rv320	-	All	All	All
Operating System	Cisco	Rv320 Firmware	All	All	All	All
Hardware	Cisco	Rv325	-	All	All	All

Hardware	Cisco	Rv325	-	All	All	All
Operating System	Cisco	Rv325 Firmware	All	All	All	All

cpe:2.3:h:cisco:rv016:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:rv016:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:rv016_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:rv042:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:rv042:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:rv042g:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:rv042g:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:rv042g_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:rv042_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:rv082:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:rv082:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:rv082_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:rv320:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:rv320:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:rv320_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:rv325:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:rv325:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:rv325_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report