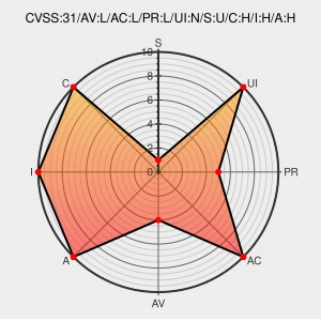
CVE-2020-3600

Published on: 11/06/2020 12:00:00 AM UTC

Last Modified on: 10/19/2021 02:43:00 PM UTC

CVE-2020-3600 - advisory for cisco-sa-vepeshlg-tJghOQcA

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



Certain versions of Sd-wan from Cisco contain the following vulnerability:

A vulnerability in Cisco SD-WAN Software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient security controls on the CLI. An attacker could exploit this vulnerability by using an affected CLI utility that is running on an affected system. A successful exploit could allow the attacker to gain root privileges.

CVE-2020-3600 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 not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco SD-WAN Solution** version **n/a**

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Cisco SD-WAN Software Privilege Escalation Vulnerability	Patch Vendor Advisory tools.cisco.com text/html	CISCO 20201104 Cisco SD-WAN Software Privilege Escalation Vulnerability

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
Application	Cisco	Sd-wan	All	All	All	All
Application	Cisco	Sd-wan	All	All	All	All

cpe:2.3:a:cisco:sd-wan:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:sd-wan:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→