

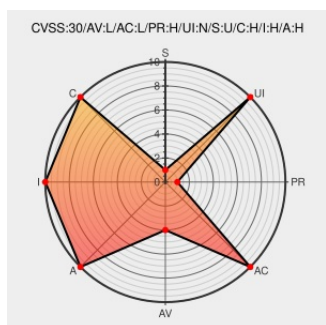


CVE-2020-3253

Published on: 05/06/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-3253 - advisory for cisco-sa-ftd-shell-9rhJF68K

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

Certain versions of [Firepower Threat Defense](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the support tunnel feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to access the shell of an affected device even though expert mode is disabled. The vulnerability is due to improper configuration of the support tunnel feature. An attacker could exploit this vulnerability by

enabling the support tunnel, setting a key, and deriving the tunnel password. A successful exploit could allow the attacker to run any system command with root access on an affected device.

CVE-2020-3253 has been assigned by [psirt@cisco.com](#) to track the vulnerability - currently rated as **MEDIUM** 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 Firepower Threat Defense Software** version n/a

CVSS3 Score: **6.7 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	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 Firepower Threat Defense Software Shell Access Vulnerability	Vendor Advisory tools.cisco.com text/html	 CISCO 20200506 Cisco Firepower Threat Defense Software Shell Access 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	Firepower Threat Defense	All	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All

cpe:2.3:a:cisco:firepower_threat_defense:*****:

cpe:2.3:a:cisco:firepower_threat_defense:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→