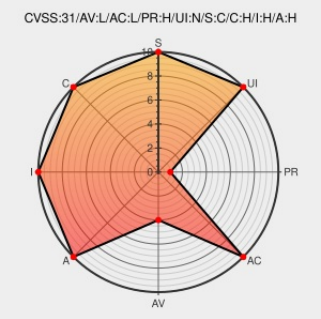
CVE-2020-3514

Published on: 10/21/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:22:00 AM UTC

CVE-2020-3514 - advisory for cisco-sa-ftd-container-esc-FmYqFBQV

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



Certain versions of Firepower Management Center from Cisco contain the following vulnerability:

A vulnerability in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their Cisco FTD instance and execute commands with root privileges in the host namespace. The attacker must have valid credentials on the device.The vulnerability exists because a configuration file that is used at container startup has insufficient protections. An attacker could exploit this vulnerability by modifying a specific container configuration file on the underlying file system. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running Cisco FTD instances or the host Cisco FXOS device.

CVE-2020-3514 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 Multi-Instance Container Escape Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20201021 Cisco Firepower Threat Defense Software Multi-Instance Container Escape Vulnerability

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 Management Center	All	All	All	All
Application	Cisco	Firepower Management Center	All	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All
Application	Cisco	Firepower Threat Defense	6.6.0	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All
Application	Cisco	Firepower Threat Defense	6.6.0	All	All	All

cpe:2.3:a:cisco:firepower_management_center:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:firepower_management_center:*:*:*:*:*:*:*:*:

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

cpe:2.3:a:cisco:firepower_threat_defense:6.6.0:*:*:*:*:*:*:*:

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

cpe:2.3:a:cisco:firepower_threat_defense:6.6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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