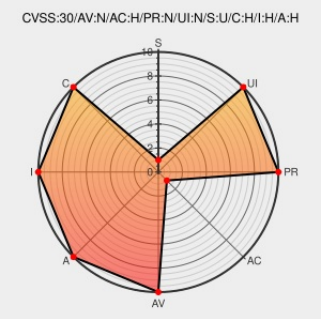
CVE-2020-3549

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

Last Modified on: 03/23/2021 11:23:39 PM UTC

CVE-2020-3549 - advisory for cisco-sa-ftdfmc-sft-mitm-tc8AzFs2

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



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

A vulnerability in the sftunnel functionality of Cisco Firepower Management Center (FMC) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to obtain the device registration hash. The vulnerability is due to insufficient sftunnel negotiation protection during initial device registration. An attacker in a man-in-the-middle position could exploit this vulnerability by intercepting a specific flow of the sftunnel communication between an FMC device and an FTD device. A successful exploit could allow the attacker to decrypt and modify the sftunnel communication between FMC and FTD devices, allowing the attacker to modify configuration data sent from an FMC device to an FTD device or alert data sent from an FTD device to an FMC device.

CVE-2020-3549 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 Firepower Management Center** version **n/a**

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Cisco Firepower Management Center Software and Firepower Threat Defense Software sftunnel Pass the Hash Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20201021 Cisco Firepower Management Center Software and Firepower Threat Defense Software sftunnel Pass the Hash 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	All	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:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→