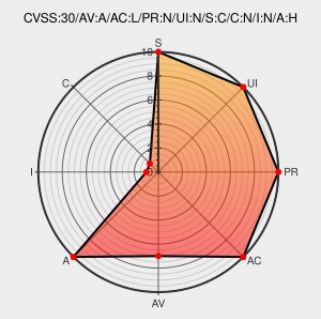
CVE-2020-3577

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

Last Modified on: 10/19/2021 02:46:00 PM UTC

CVE-2020-3577 - advisory for cisco-sa-ftd-inline-dos-nXqUyEqM

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



Certain versions of Firepower Threat Defense from Cisco contain the following vulnerability:

A vulnerability in the ingress packet processing path of Cisco Firepower Threat Defense (FTD) Software for interfaces that are configured either as Inline Pair or in Passive mode could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient validation when Ethernet frames are processed. An attacker could exploit this vulnerability by sending malicious Ethernet frames through an affected device. A successful exploit could allow the attacker do either of the following: Fill the /ngfw partition on the device: A full /ngfw partition could result in administrators being unable to log in to the device (including logging in through the console port) or the device being unable to boot up correctly. Note: Manual intervention is required to recover from this situation. Customers are advised to contact the Cisco Technical Assistance Center (TAC) to help recover a device in this condition. Cause a process crash: The process crash would cause the device to reload. No manual intervention is necessary to recover the device after the reload.

CVE-2020-3577 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 Threat Defense Software** version **n/a**

CVSS3 Score: 7.4 - HIGH

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

CVSS2 Score: 6.1 - MEDIUM

CVSS2 Score: 6.1 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Cisco Firepower Threat Defense Software Inline Pair/Passive Mode Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20201021 Cisco Firepower Threat Defense Software Inline Pair/Passive Mode Denial of Service 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 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

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→