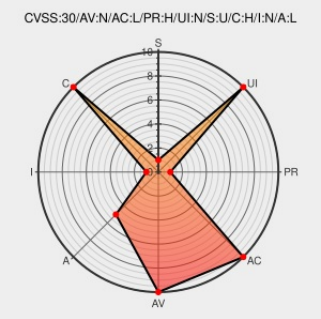
CVE-2020-3310

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

Last Modified on: 10/19/2021 08:06:00 PM UTC

CVE-2020-3310 - advisory for cisco-sa-xpftd-gYDXyN8H

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



Certain versions of Firepower Device Manager On-box from Cisco contain the following vulnerability:

A vulnerability in the XML parser code of Cisco Firepower Device Manager On-Box software could allow an authenticated, remote attacker to cause an affected system to become unstable or reload. The vulnerability is due to insufficient hardening of the XML parser configuration. An attacker could exploit this vulnerability in multiple ways using a malicious file: An attacker with administrative privileges could upload a malicious XML file on the system and cause the XML code to parse the malicious file. An attacker with Clientless Secure Sockets Layer (SSL) VPN access could exploit this vulnerability by sending a crafted XML file. A successful exploit would allow the attacker to crash the XML parser process, which could cause system instability, memory exhaustion, and in some cases lead to a reload of the affected system.

CVE-2020-3310 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: 4.9 - MEDIUM

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Cisco Firepower Device Manager On-Box Software XML Parsing Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20200506 Cisco Firepower Device Manager On-Box Software XML Parsing 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 Device Manager On-box	All	All	All	All
Application	Cisco	Firepower Device Manager On-box	All	All	All	All

cpe:2.3:a:cisco:firepower_device_manager_on-box:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:firepower_device_manager_on-box:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→