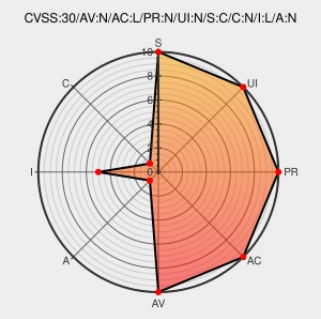
CVE-2020-3285

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

Last Modified on: 10/12/2021 01:59:00 PM UTC

CVE-2020-3285 - advisory for cisco-sa-ssl-bypass-O5tGum2n

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



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

A vulnerability in the Transport Layer Security version 1.3 (TLS 1.3) policy with URL category functionality for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass a configured TLS 1.3 policy to block traffic for a specific URL. The vulnerability is due to a logic error with Snort handling of the connection with the TLS 1.3 policy and URL category configuration. An attacker could exploit this vulnerability by sending crafted TLS 1.3 connections to an affected device. A successful exploit could allow the attacker to bypass the TLS 1.3 policy and access URLs that are outside the affected device and normally would be dropped.

CVE-2020-3285 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: 5.8 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco Firepower Threat Defense Software SSL/TLS URL Category Bypass Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20200506 Cisco Firepower Threat Defense Software SSL/TLS URL Category Bypass 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

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→