



CVE-2020-3565

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

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

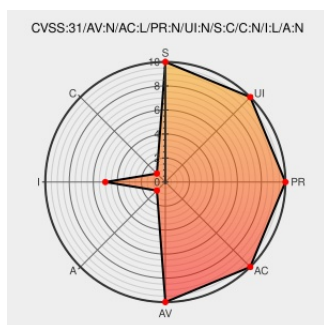
CVE-2020-3565 - advisory for cisco-sa-tcp-intercept-bypass-xG9M3PbY

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Firepower Threat Defense](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the TCP Intercept functionality of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured Access Control Policies (including Geolocation) and Service Policies on an affected system.

The vulnerability exists because TCP Intercept is invoked when the embryonic connection limit is reached, which can cause the underlying detection engine to process the packet incorrectly. An attacker could exploit this vulnerability by sending a crafted stream of traffic that matches a policy on which TCP Intercept is configured. A successful exploit could allow the attacker to match on an incorrect policy, which could allow the traffic to be forwarded when it should be dropped. In addition, the traffic could incorrectly be dropped.

CVE-2020-3565 has been assigned by [Cisco](#) 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 - 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: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

Cisco Firepower Threat Defense Software TCP Intercept Bypass Vulnerability

Vendor Advisory

tools.cisco.com

text/html

CISCO 20201021

Cisco Firepower Threat Defense Software TCP Intercept Bypass Vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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

← Previous ID

Next ID →