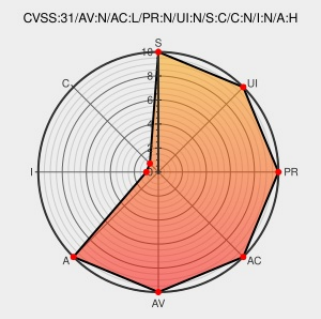
CVE-2020-3572

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

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

CVE-2020-3572 - advisory for cisco-sa-asa-ftd-tcp-dos-N3DMnU4T

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



Certain versions of Adaptive Security Appliance from Cisco contain the following vulnerability:

A vulnerability in the SSL/TLS session handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a memory leak when closing SSL/TLS connections in a specific state. An attacker could exploit this vulnerability by establishing several SSL/TLS sessions and ensuring they are closed under certain conditions. A successful exploit could allow the attacker to exhaust memory resources in the affected device, which would prevent it from processing new SSL/TLS connections, resulting in a DoS. Manual intervention is required to recover an affected device.

CVE-2020-3572 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 Adaptive Security Appliance (ASA) Software** version **n/a**

CVSS3 Score: 8.6 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software SSL/TLS Session Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20201021 Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software SSL/TLS Session 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	Adaptive Security Appliance	All	All	All	All
Application	Cisco	Adaptive Security Appliance	All	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	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:adaptive_security_appliance:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*:

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→

CVE.report and Source URL Uptime Status status.cve.report