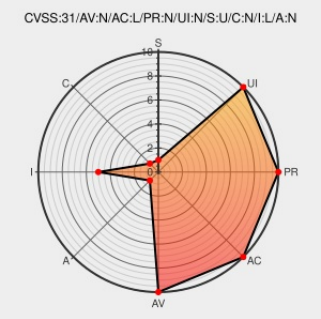
CVE-2020-3578

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

Last Modified on: 05/26/2022 03:11:00 PM UTC

CVE-2020-3578 - advisory for cisco-sa-asaftd-rule-bypass-P73ABNWQ

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



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

A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass a configured access rule and access parts of the WebVPN portal that are supposed to be blocked. The vulnerability is due to insufficient validation of URLs when portal access rules are configured. An attacker could exploit this vulnerability by accessing certain URLs on the affected device.

CVE-2020-3578 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 Adaptive Security Appliance (ASA) Software** version **n/a**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software WebVPN Portal Access Rule Bypass Vulnerability	Patch Vendor Advisory tools.cisco.com text/html	CISCO 20201021 Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software WebVPN Portal Access Rule Bypass Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Adaptive Security Appliance Software	All	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	All	All	All	All
Operating System	Cisco	Firepower Threat Defense	All	All	All	All
Operating System	Cisco	Firepower Threat Defense	All	All	All	All

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

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

cpe:2.3:o:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? | A vulnerability in the web services inte... | CVE-2020-3578 | Link for more: alerts.remotelyrmm.com/CVE-2020-3578	2022-05-26 16:28:55

← Previous ID

Next ID→

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