

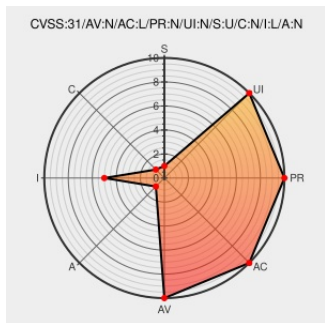


CVE-2020-3578

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-asafth-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 [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 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			
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
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 →			

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)