

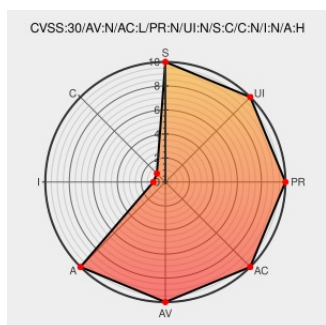


CVE-2020-3304

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

Last Modified on: 08/16/2023 04:17:00 PM UTC

CVE-2020-3304 - advisory for cisco-sa-asafld-webdos-fBzM5Ynw

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Adaptive Security Appliance](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the web interface of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to a lack of proper input

validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. An exploit could allow the attacker to cause a DoS condition. Note: This vulnerability applies to IP Version 4 (IPv4) and IP Version 6 (IPv6) HTTP traffic.

CVE-2020-3304 has been assigned by [Cisco](#) 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: **7.8 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	Integrity	Availability

Impact		Impact		Impact		
NONE		NONE		COMPLETE		
CVE References						
Description		Tags		Link		
Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Denial of Service Vulnerability		Vendor Advisory tools.cisco.com text/html		 CISCO 20201021 Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Denial of Service 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	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→				

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](#)