



CVE-2020-3436

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

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

CVE-2020-3436 - advisory for cisco-sa-asafld-fileup-dos-zvC7wtys

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H



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

A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to upload arbitrary-sized files to specific folders on an affected device, which could lead to an unexpected device reload. The vulnerability exists because the

affected software does not efficiently handle the writing of large files to specific folders on the local file system. An attacker could exploit this vulnerability by uploading files to those specific folders. A successful exploit could allow the attacker to write a file that triggers a watchdog timeout, which would cause the device to unexpectedly reload, causing a denial of service (DoS) condition.

CVE-2020-3436 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 - 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 Impact

Integrity Impact

Availability Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services File Upload 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 File Upload 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	6.6.0	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All
Application	Cisco	Firepower Threat Defense	6.6.0	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:6.6.0:*:*:*:*:*:						
cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:						
cpe:2.3:a:cisco:firepower_threat_defense:6.6.0:*:*:*:*:*:						
cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)