



CVE-2018-15399

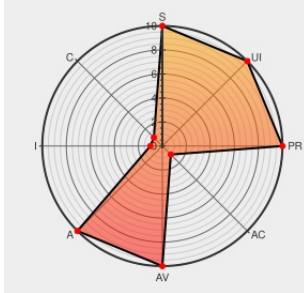
Published on: 10/05/2018 12:00:00 AM UTC

Last Modified on: 08/15/2023 03:21:00 PM UTC

CVE-2018-15399 - advisory for cisco-sa-20181003-asa-syslog-dos

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

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H



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

A vulnerability in the TCP syslog module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to exhaust the 1550-byte buffers on an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing boundary check in an internal function. An attacker could exploit this vulnerability by establishing a man-in-the-middle position between an affected device and its configured TCP syslog server and then maliciously modifying the TCP header in segments that are sent from the syslog server to the affected device. A successful exploit could allow the attacker to exhaust buffer on the affected device and cause all TCP-based features to stop functioning, resulting in a DoS condition. The affected TCP-based features include AnyConnect SSL VPN, clientless SSL VPN, and management connections such as Secure Shell (SSH), Telnet, and HTTPS.

CVE-2018-15399 has been assigned by [psirt@cisco.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Cisco](#) - **Cisco Adaptive Security Appliance (ASA) Software** version n/a

CVSS3 Score: **6.8 - MEDIUM**

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

CVSS2 Score: **7.1 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

Cisco ASA Bug in TCP Syslog Module Lets Remote Users Cause the Target Service to Crash - SecurityTracker

Third Party Advisory

VDB Entry

www.securitytracker.com

text/html

SECTRAK 1041785

Cisco Adaptive Security Appliance TCP Syslog Denial of Service Vulnerability

Vendor Advisory

tools.cisco.com

text/html

CISCO 20181003 Cisco Adaptive Security Appliance TCP Syslog 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 Software

9.4(4)

All

All

All

Application

Cisco

Adaptive Security Appliance Software

9.4\ (4)

All

All

All

Application

Cisco

Adaptive Security Appliance Software

9.8(2)

All

All

All

Application

Cisco

Adaptive Security Appliance Software

9.8\ (2)

All

All

All

Operating System

Cisco

Adaptive Security Appliance Software

9.4\ (4)

All

All

All

Operating System

Cisco

Adaptive Security Appliance Software

9.8\ (2)

All

All

All

Application

Cisco

Adaptive Security Appliance Software

9.4\ (4)

All

All

All

Application

Cisco

Adaptive Security Appliance Software

9.8\ (2)

All

All

All

Application

Cisco

Firepower Threat Defense

6.2.0

All

All

All

Application

Cisco

Firepower Threat Defense

6.2.0

All

All

All

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.4(4):*:~::~

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.4\ (4):*:~::~

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.8(2):*:~::~

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.8\ (2):*:~::~

cpe:2.3:o:cisco:adaptive_security_appliance_software:9.4(4):*:~::~

cpe:2.3:o:cisco:adaptive_security_appliance_software:9.8\ (2):*:~::~

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.4(4):*****:
cpe:2.3:a:cisco:adaptive_security_appliance_software:9.8(2):*****:
cpe:2.3:a:cisco:firepower_threat_defense:6.2.0:*****:
cpe:2.3:a:cisco:firepower_threat_defense:6.2.0:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→