

CVE-2018-0296

Cisco Adaptive Security Appliance (ASA) Denial-of-Service Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

A vulnerability in the web interface of the Cisco Adaptive Security Appliance (ASA) could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. It is also possible on certain software releases that the ASA will not reload, but an attacker could view sensitive system information without authentication by using directory traversal techniques. The vulnerability is due to lack of proper input validation of the HTTP URL.

EVRS 84/100 Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.999 99.97th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · listed over a year
---	--	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

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 or unauthenticated disclosure of information. This vulnerability applies to IPv4 and IPv6 HTTP traffic. This vulnerability affects Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software that is running on the following Cisco products: 3000 Series Industrial Security Appliance (ISA), ASA 1000V Cloud Firewall, ASA 5500 Series Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls, ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, Adaptive Security Virtual Appliance (ASAv), Firepower 2100 Series Security Appliance, Firepower 4100 Series Security Appliance, Firepower 9300 ASA Security Module, FTD Virtual (FTDv). Cisco Bug IDs: CSCvi16029.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
firepower threat defense	6.2.3-85.02 6.2.3-851	no fixed version listed	NVD
secure firewall threat defense	≥ 6.0 < 6.1.0 ≥ 6.2.1 < 6.2.2.3 6.2.3 6.2.3.1	no fixed version listed	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
adaptive security appliance software	≥ 9.1 < 9.1.7.29	9.1.7.29 · 9.2.4.33 ·	NVD
	≥ 9.2 < 9.2.4.33	9.4.4.18 · 9.6.4.8 · 9.7.1.24	
	≥ 9.3 < 9.4.4.18	· 9.8.2.28	
	≥ 9.5 < 9.6.4.8		
	≥ 9.7 < 9.7.1.24		
	≥ 9.8 < 9.8.2.28		
	≥ 9.9 < 9.9.2.1		

Sources

Vendor guidance github.com/advisories/GHSA-h2mj-pqgp-xmmj

Additional guidance tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-asaftd

NVD nvd.nist.gov/vuln/detail/CVE-2018-0296

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-1119

Current data evulnable.com/vulnerability-management/cve/CVE-2018-0296

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.