SECURITYWEEK NETWORK:

- Cybersecurity News
- Infosec Island
- Virtual Events

Security Experts:

WRITE FOR US

SECURITY WEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe
- 2021 CISO Forum
- ICS Cyber Security Conference
- Contact

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Threat Intelligence
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance

Cisco Patches High-Severity DoS Vulnerabilities in ASA, FTD Software

By Ionut Arghire on October 28, 2021

Cisco this week announced the release of a new set of security patches to address multiple vulnerabilities affecting Adaptive Security Appliance (ASA), Firepower Threat Defense (FTD), and Firepower Management Center (FMC) software.

A dozen of the security errors, all of which were addressed as part of the October 2021 ASA, FTD, and FMC Security Advisory Bundled publication, carry a *high severity* rating. Most of these can be exploited to achieve a denial of service (DoS) condition, some without authentication.

The most severe of the addressed vulnerabilities is CVE-2021-40116 (CVSS score of 8.6), a security error in Snort rules that could be exploited remotely, without authentication, to cause a DoS condition on an affected device.

The issue, Cisco explains, exists because of “improper handling of the Block with Reset or Interactive Block with Reset actions if a rule is configured without proper constraints.” An attacker could send crafted IP packets to exploit this flaw and cause traffic to be dropped.

The vulnerability affects only products that have Snort3 and a rule with Block with Reset or Interactive Block with Reset actions configured. All open source Snort3 project releases prior to 3.1.0.100 are vulnerable.

Another severe issue addressed this week is CVE-2021-34783 (CVSS score of 8.6), an insufficient validation of SSL/TLS messages during software-based SSL/TLS decryption. By sending crafted SSL/TLS messages, an attacker could cause the affected device to reload.

This week, Cisco also released patches for multiple vulnerabilities in the CLI of FTD, which could be exploited by a local, authenticated attacker to achieve code execution as root.

Other high-severity issues Cisco patched this week include improper error handling in the processing of SSH connections in FTD, directory traversal attack in FMC, and several bugs affecting both ASA and FTD: improper processing of SSL/TLS packets, improper input validation during the parsing of HTTPS requests, improper resource management at high connection rates, and incorrect handling of certain TCP segments.

In addition to these high-severity issues, Cisco this week patched over a dozen medium-severity security holes in ASA and FTD, including flaws that could lead to DoS conditions, the bypass of ALG or other security protections, overwrite of data with root privileges, information leak, or cross-site scripting (XSS) attacks.

Cisco says it is not aware of any of these vulnerabilities being exploited in the wild.

Patches were released for all of these vulnerabilities and, in some cases, workarounds are also available. Further information on the bugs can be found on Cisco's security portal.

Related: Cisco Patches High-Severity Vulnerabilities in Security Appliances, Business Switches

Related: Cisco Patches Critical Vulnerabilities in IOS XE Software

Related: Cisco Patches High-Severity Security Flaws in IOS XR

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

FBI Publishes Indicators of Compromise for Ranzy Locker Ransomware
Vendor-Neutral Initiative Sets Bare-Minimum Baseline for Security
Phishing Protection Provider SlashNext Raises $26 Million
Cisco Patches High-Severity DoS Vulnerabilities in ASA, FTD Software
Washington Secretary of State Appointed CISA's Senior Election Security Lead

Tags:

NEWS & INDUSTRY Vulnerabilities