Security Advisory 2021-058

Multiple Severe Vulnerabilities in Cisco Products

October 29, 2021 — v1.0

TLP:WHITE

History:

- *29/10/2021 — v1.0 – Initial publication*

Summary

On October 27, Cisco released multiple security fixes about vulnerabilities affecting their products, including nine with a high CVSS score. These vulnerabilities affect the open source Snort3 project, Adaptive Security Appliance (ASA), Firepower Threat Defense (FTD) and Firepower Management Center software (FMC) [1].

Technical Details

CVE-2021-40116 - Snort Rule Denial of Service Vulnerability

This vulnerability with a CVSS score of 8.6 out of 10 affects multiple Cisco products running Snort3 releases earlier than `Release 3.1.0.100`, configured with `Block with Reset` or `Interactive Block with reset` actions. It is due to improper handling of these actions, if one of the rules is not configured with proper constraints. A remote, unauthenticated attackers could exploit this vulnerability by sending a crafted IP packet to the products running Snort3 that will cause traffic to be dropped (DoS condition). [2]

This vulnerability does not affect Snort2 configurations and the following products:

- Adaptive Security Appliance (ASA) Software
- 1000 Series Integrated Services Routers (ISRs)
- 4000 Series Integrated Services Routers (ISRs)
- Catalyst 8000V Edge Software
- Catalyst 8200 Series Edge Platforms
- Catalyst 8300 Series Edge Platforms
- Catalyst 8500 Series Edge Platforms
- Catalyst 8500L Series Edge Platforms
- Cloud Services Router 1000V Series
- Firepower Management Center (FMC) Software
- Integrated Services Virtual Router (ISRv)
- Meraki Security Appliances

Workaround

Cisco proposes to change the Snort inspection engine from Snort3 to Snort2, or change all rule actions with `Block with Reset` or `Interactive block with Reset` to another action. Another Workaround proposed by Cisco consists in changing the firewall reset rule by narrowing the configuration rule, or by setting up the application or the protocol.

CVE-2021-34783 - ASA and FTD Software-Based SSL/TLS Denial of Service Vulnerability

This vulnerability with a CVSS score of 8.6 out of 10 affects ASA and FTD software, allowing an unauthenticated, remote attacker to cause a Denial of Service condition. This is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. To exploit this vulnerability, an attacker could craft and send an SSL/TLS message to an affected device, causing the reload and the DoS condition. [3]

CVE-2021-34781 - FTD SSH Connections Denial of Service Vulnerability

This vulnerability with a CVSS score of 8.6 out of 10 affects FTD software, allowing a unauthenticated, remote attacker to cause a Denial of Service condition on the device. This is due to the lack of proper error handling when an SSH session fails to be established. To exploit the vulnerability, an attacker could send a high rate of crafted SSH connections to the device, causing a resource exhaustion, and at the same time, a Denial of Service condition on the device, which should be reloaded to recover [4].

CVE-2021-34752/CVE-2021-34755/CVE-2021-34756 - FTD Command Injection Vulnerabilities

These vulnerabilities with a CVSS score of 7.8 out of 10 affect the Cisco FTD software, allowing an authenticated, local attacker to execute arbitrary commands with root privileges. This is due to multiple vulnerabilities in the CLI of Cisco FTD Software, more precisely to insufficient validation of user-supplied command arguments. To exploit this vulnerability, an attacker could submit a crafted input to execute command with root privileges on the underlying operating system. [8]

Depending on the configuration of the device running the vulnerable release, it might be affected by distinct CVEs:

Cisco FTD Configuration	Associated CVE IDs
Multi-instance	CVE-2021-34755 and CVE-2021-34756
Default	CVE-2021-34752

CVE-2021-34762 - FMC Authenticated Directory Traversal Vulnerability

This vulnerability with a CVSS score of 8.1 out of 10 affects FMC software, allowing an authenticated, remote attacker to perform directory traversal attack. It is due to insufficient input validation of the HTTPS URL by the web-based management interface. To exploit this vulnerability, an attacker could send crafted HTTPS request that contains directory traversal character sequence, allowing the attacker to read or write arbitrary files on the device. [5]

CVE-2021-40117 - ASA and FTD SSL/TLS Denial of Service Vulnerability

This vulnerability with a CVSS score of 8.6 out of 10 affects ASA and FTD software, and allows an unauthenticated, remote attacker to cause a Denial of Service condition. It exists because incoming SSL/TLS packets are not properly processed. To exploit this vulnerability, an attacker could craft and send an SSL/TLS message to an affected device, causing the reload and the DoS condition of it. [6]

CVE-2021-1573/CVE-2021-34704/CVE-2021-40118 - ASA and FTD Web Services Denial of Service Vulnerabilities

These vulnerabilities with a CVSS score of 8.6 out of 10 affects ASA and FTD software, and allow an unauthenticated, remote attacker to cause a Denial of Service condition. This is due to improper input validation when parsing HTTPS requests. To exploit this vulnerability, an attacker could send malicious HTTPS request to an affected device, leading to the reload of the device, causing a Denial of Service [7].

CVE-2021-34792 - ASA and FTD Resource Exhaustion Denial of Service Vulnerability

This vulnerability with a CVSS score of 8.6 affects ASA and FTD software, and allows an unauthenticated, remote attacker to cause a Denial of Service condition. This is due to improper resource management when connection rates are high. To exploit this vulnerability, an attacker could open a significant number of connections on an affected device, leading to the reload of the device, causing a Denial of Service condition [9].

CVE-2021-34793 - ASA and FTD Transparent Mode Denial of Service Vulnerability

This vulnerability with a CVSS score of 8.6 affects ASA and FTD software, allowing an unauthenticated, remote attacker to cause a Denial of Service condition. It is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. To exploit this vulnerability, an attacker could send a crafted TCP segment through an affected device, allowing the attacked to poison the MAC address tables in adjacent devices, resulting in network disruption [10].

Affected Products and Fixed Releases

- Cisco ASA Software

Cisco ASA Software Release	Fixed Release for All Vulnerabilities Described in the Advisory
9.7 and earlier	Migrate to a fixed release.
9.8	9.8.4.40
9.9	Migrate to a fixed release.
9.10	Migrate to a fixed release.
9.12	9.12.4.29
9.13	Migrate to a fixed release.
9.14	9.14.3.9
9.15	9.15.1.17
9.16	9.16.2.3

- Cisco FTD Software

Cisco FTD Software Release	Fixed Release for All Vulnerabilities Described in the Advisory
6.2.2 and earlier	Migrate to a fixed release.
6.2.3	Migrate to a fixed release.
6.3.01	Migrate to a fixed release.
6.4.0	6.4.0.13 (Nov 2021)
6.5.0	Migrate to a fixed release.
6.6.0	6.6.5.1 (Nov 2021)
6.7.0	6.7.0.3 (Jan 2022)
7.0.0	7.0.1

Recommendations

To fix all these vulnerabilities, CERT-EU and Cisco highly recommend updating each release to the last version, when possible, or to upgrade the release.

References

[1] https://tools.Cisco.com/security/center/viewErp.x?alertId=ERP-74773

[2] https://tools.Cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-sa-snort-dos-RywH7ezM

[3] https://tools.Cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M

[4] https://tools.Cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-sa-ftd-dos-rUDseW3r

[5] https://tools.Cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-sa-fmc-dir-traversal-95UyW5tk

[6] https://tools.Cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-sa-asaftd-dos-4ygzLKU9

[7] https://tools.Cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-sa-asafdt-webvpn-dos-KSqJAKPA

[8] https://tools.Cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-sa-ftd-cmdinject-FmzsLN8

[9] https://tools.Cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-sa-asa-ftd-dos-Unk689XY

[10] https://tools.Cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-sa-asa-ftd-dos-JxYWMJyL