

Alert Bulletin

Bulletin N.: 120

Publication Date: 22/10/2026

Subject: Alert 2026-120 Critical vulnerabilities in Cisco Snort 3 affect FTD, Cyber Vision, and other products

Traffic Light Protocol (TLP): White

Affected product(s):

Product	Affected versions
Open Source Snort 3	Earlier than 3.12.4.0
Cisco Secure Firewall Threat Defense (FTD)	Earlier than 7.0.10, 7.2.12, 7.4.8, 7.6.6, 7.7.13, and 10.0.2
UTD on Cisco IOS XE	Earlier than 17.12.8, 17.15.6, 17.18.5, 26.1.2, and 26.2.1
Cisco Cyber Vision	Earlier than 5.6.0
Cisco Meraki MX	Devices without the updated Snort 3 package
Cisco Cloud-delivered Firewall and Secure Access	Updated by Cisco on 21/10/2026

They are affected regardless of configuration. Open Source Snort 2 is not affected.

Description

A critical out-of-bounds write vulnerability (CWE-787) has been disclosed in Cisco's Snort 3 inspection engine, identified as CVE-2026-20043 (CVSSv3.1 9.0 – CRITICAL), affecting Open Source Snort 3 and Cisco products that integrate it, including Secure Firewall Threat Defense (FTD), Cyber Vision, Meraki MX, UTD on IOS XE, Cloud-delivered Firewall, and Secure Access.

The flaw was disclosed on October 21, 2026 as part of a Snort 3 hardening (security hardening) release that fixes multiple vulnerabilities discovered by the Snort 3 engineering team itself during an internal review. Cisco grouped the flaws by weakness class (CWE) and assigned a single CVE to each group. The score for each CVE corresponds to the most severe vulnerability in its group.

The CVE-2026-20043 vector (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H) indicates that it can be exploited over the network without authentication or user interaction, although with high complexity. A successful attack could compromise confidentiality, integrity, and availability, with scope extending beyond

the vulnerable component. Cisco does not describe the specific Snort 3 components affected or the technical conditions for exploitation.

The same advisory includes three other vulnerability groupings:

CVE	Maximum CVSS score (Cisco advisory)	CWE	Vulnerability class
CVE-2026-20043	9.0	CWE-787	Out-of-bounds write
CVE-2026-20236	9.0	CWE-682	Incorrect calculation
CVE-2026-20291	7.8 (local vector, requires low privileges)	CWE-269	Improper Privilege Management
CVE-2026-20356	7.5	CWE-400	Uncontrolled resource consumption (denial of service)

Cisco PSIRT is not aware of any public announcements or malicious exploitation of these vulnerabilities. According to the vendor, they were discovered through internal security testing that combined existing testing processes with frontier AI models.

Solution

Cisco recommends updating to the fixed versions of each product and states that there are no workarounds to prevent these vulnerabilities. Because of their traffic inspection function, priority should be given to perimeter appliances (FTD, UTD on IOS XE routers) and self-managed Snort 3 sensors.

Cisco Secure Firewall Threat Defense (FTD)

Cisco Secure FTD branch First fixed version

7.0 and earlier	7.0.10
7.2	7.2.12
7.4	7.4.8
7.6	7.6.6
7.7	7.7.13
10.0	10.0.2
10.1	10.1.0

Unified Threat Defense (UTD) on Cisco IOS XE

The following Cisco IOS XE UTD images include Open Source Snort 3 version 3.12.4.0 (table updated by Cisco on 22/10/2026, version 1.1 of the advisory):

Cisco IOS XE branch First fixed version (UTD image)

17.12	17.12.8 (secapp-utd.17.12.08.1.2.8_SV3.12.4.0_XE17.12)
17.15	17.15.6 (secapp-utd.17.15.06.1.0.21_SV3.12.4.0_XE17.15)
17.18	17.18.5
26.1	26.1.2 (secapp-utd.26.01.02.1.0.6_SV3.12.4.0_XE26.1)
26.2	26.2.1

Open Source Snort 3, Cyber Vision, and managed services

Product	Branch	Action / fixed version
Open Source Snort 3	3.x	Update to 3.12.4.0
Cisco Cyber Vision	Earlier than 5.6	Migrate to a fixed version
Cisco Cyber Vision	5.6	5.6.0
Cisco Meraki MX	—	No action: Cisco automatically updated the Snort 3 package on 21/10/2026 on online appliances connected to Meraki Dashboard
Cisco CDFW and CSA	—	No action: cloud instances updated by Cisco on 21/10/2026

For Meraki MX, verify in Meraki Dashboard that there are no disconnected or offline appliances that have not received the fixed Snort 3 package.

Cisco Secure Firewall Threat Defense / Management Center upgrade guides:

<https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-guides-list.html>

Open Source Snort 3 version 3.12.4.0:

<https://github.com/snort3/snort3/releases/tag/3.12.4.0>

Additional information:

- Cisco PSIRT — Multiple Cisco Products Snort 3 Security Hardening Release: October 2026: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-snort3-ybgmhTQe>
- Cisco PSIRT — advance notification of the October 21, 2026 advisories (related Snort 3 advisories): <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-notice-QGwHnJ6k>
- NVD — CVE-2026-20043: <https://nvd.nist.gov/vuln/detail/CVE-2026-20043>
- NVD — CVE-2026-20236: <https://nvd.nist.gov/vuln/detail/CVE-2026-20236>
- NHS England Digital — CC-4878, Cisco Releases Security Hardening Guidance for Multiple Cisco Products: <https://digital.nhs.uk/cyber-alerts/2026/cc-4878>
- Snort 3 — release 3.12.4.0 (GitHub): <https://github.com/snort3/snort3/releases/tag/3.12.4.0>