Cisco Snort 3 DCE/RPC Vulnerabilities Impact Multiple Security Platforms

TL;DR

Cisco patched two Snort 3 DCE/RPC vulnerabilities (CVE-2026-20026 and CVE-2026-20027) that could allow a remote attacker to crash the Snort 3 detection engine or leak sensitive inspection data.

If you are running Snort 3 on Cisco Secure Firewall Threat Defense (FTD), Cisco IOS XE with UTD, Open Source Snort 3, or certain Meraki MX devices, review your version and patch.

Overview

Cisco released updates addressing two medium-severity vulnerabilities in the Snort 3 Detection Engine related to improper handling of Distributed Computing Environment / Remote Procedure Call (DCE/RPC) traffic. These vulnerabilities do not affect the core firewall functionality itself, but they do impact the Snort 3 inspection engine embedded within certain Cisco firewall and security platforms, which could interrupt traffic inspection or expose inspection-related data if exploited.

Impacted Products

These vulnerabilities affect the following products only when Snort 3 is active or integrated:

- Open Source Snort 3 (prior to 3.9.6.0)
- Cisco Secure Firewall Threat Defense (FTD) Software running Snort 3
- Cisco IOS XE Software with Unified Threat Defense (UTD) Snort IPS Engine enabled
- Cisco IOS XE SD-WAN Software with UTD Engine enabled
- Cisco Meraki MX models with integrated Snort 3

Not affected:

- Open Source Snort 2
- Cisco Secure Firewall ASA Software
- Cisco Secure Firewall Management Center (FMC) Software
- Cisco Umbrella Cloud-delivered Firewall
- Cisco Cyber Vision

CVE-2026-20026 (CVSS 5.8)

This vulnerability stems from flawed buffer handling logic that can trigger a use-after-free read condition when Snort 3 processes DCE/RPC requests. An unauthenticated remote attacker could send specially crafted DCE/RPC traffic through an established connection being inspected by Snort 3. Successful exploitation could force the Snort 3 engine to restart, interrupting packet inspection and creating a temporary blind spot in network visibility.

CVE-2026-20027 (CVSS 5.3)

This issue results from an out-of-bounds read condition in the DCE/RPC processing logic. A remote attacker could send crafted DCE/RPC requests that cause Snort 3 to expose portions of sensitive data within the inspection stream. While this does not provide code execution, it may disclose information that should remain internal to the inspection process.

The vulnerabilities are independent and have not been exploited. Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch** – Upgrade to Snort 3 version 3.9.6.0 or later if using Open Source Snort.
- Apply Cisco Secure FTD hot fixes for affected 7.0 and 7.2 releases.
- Upgrade Cisco IOS XE Software to the first fixed release (e.g., 17.12.7, 17.15.5, 17.18.3, or 26.1.1 depending on branch). See Cisco's advisory for more information.
- Verify whether Snort 3 is active on Cisco Secure FTD deployments.
- Confirm whether UTD is enabled on Cisco IOS XE devices using show utd engine standard status.
- Review logging to ensure no inspection interruptions occurred prior to patching.

TTPs to Watch

Impact

- Endpoint Denial of Service [T1499] – The attacker may send crafted DCE/RPC traffic to force the Snort 3 engine to restart, interrupting inspection.

Collection

- Data from Local System [T1005] – The attacker may retrieve sensitive data exposed from Snort 3 memory through an out-of-bounds read condition.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

These vulnerabilities impact organizations that rely on Cisco security appliances and Snort-based inspection, including:

- Finance
- Government
- Education
- Energy
- Healthcare
- Retail
- Technology
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Multiple Cisco Products Snort 3 Distributed Computing Environment/Remote Procedure Call Vulnerabilities