Cisco Snort 3 DCE/RPC Vulnerabilities Disrupt Packet Inspection and Leak Data

TL;DR

Cisco patched two Snort 3 vulnerabilities (CVE-2026-20026 and CVE-2026-20027) that allow a remote, unauthenticated attacker to crash the inspection engine or leak data by abusing DCE/RPC traffic.

Any environment running Snort 3 (including Secure Firewall FTD, IOS XE with UTD, and Meraki MX) should review exposure and apply updates or hot fixes.

Overview

Cisco has two medium-severity vulnerabilities (CVE-2026-20026 and CVE-2026-20027) that impact Snort 3's handling of DCE/RPC traffic. Both vulnerabilities can disrupt packet inspection or expose internal data. An attacker does not need credentials or user interaction and can trigger the issues remotely by sending crafted DCE/RPC requests through an inspected connection.

Both flaws are within the Snort 3 detection engine itself. Successful exploitation could restart the engine, creating blind spots in network visibility, or leak sensitive information from the Snort data stream. Cisco has released fixes, and there are no mitigation steps besides patching.

Affected Products

- Open Source Snort 3 (versions prior to 3.9.6.0)
- Cisco Secure Firewall Threat Defense (FTD) when Snort 3 is active
- Cisco IOS XE devices running Unified Threat Defense (UTD), including ISR and Catalyst 8000 platforms
- Cisco Meraki MX appliances running vulnerable firmware

***Note**: Snort 2 deployments are not impacted. Devices without UTD installed are not affected.*

Vulnerability Breakdown

CVE-2026-20026 (CVSS 5.8) – Snort 3 DCE/RPC Denial of Service

- This issue stems from a memory handling flaw when Snort 3 processes DCE/RPC requests. Under sustained or specially crafted traffic, the engine may access freed memory and unexpectedly restart. While this does not grant code execution, it interrupts packet inspection and weakens monitoring at the network edge.

CVE-2026-20027 (CVSS 5.3) – Snort 3 DCE/RPC Information Disclosure

- A separate bounds-checking error in the same DCE/RPC processing path can expose portions of Snort 3 memory. An attacker could retrieve sensitive data from the inspection stream by sending repeated DCE/RPC requests through an established connection.

The vulnerabilities are independent and may affect systems differently depending on configuration and software version. If exploited, CVE-2026-20026 and CVE-2026-20027 can expose internal traffic data or disrupt packet inspection. This can leave a businesses with reduced network visibility and increase the chance that malicious activity slips through the cracks unnoticed. Although the vulnerability is not being exploited in the wild, Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch** – Upgrade Open Source Snort to version 3.9.6.0 or later. See Cisco's advisory for details.
- For IOS XE environments, plan upgrades to fixed versions starting with 26.1.1 (February 2026).
- Track Meraki firmware updates scheduled for February 2026 and patch promptly once available.
- Confirm whether Snort 3 or UTD is active in your environment to accurately assess exposure.

TTPs

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may send crafted DCE/RPC traffic through exposed or internet-facing devices where Snort 3 is actively inspecting network connections. No authentication is required, and exploitation relies solely on malformed protocol traffic reaching the inspection engine.

Impact

- Endpoint Denial of Service [T1499] – By triggering a memory handling flaw, the attacker may force the Snort 3 detection engine to restart, temporarily

interrupting packet inspection and reducing network visibility while the engine recovers.

Collection

- Data from Network Traffic [T1040] – In the information disclosure scenario, the attacker may extract unintended memory content from the Snort 3 inspection stream by abusing out-of-bounds reads during DCE/RPC processing.

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

Organizations using Cisco security and routing platforms with Snort 3 enabled are most impacted, including:

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