ADV2026_114 Cisco Security Advisory – Update 1 (February 26th, 2025)

Cisco has published a security advisory highlighting vulnerabilities in the following products on February 24th, 2026. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- Cisco Catalyst SD-WAN Controller – multiple versions
- Cisco Catalyst SD-WAN Manager – multiple versions
- Cisco Nexus 3600 and 9500-R Switching Platform – multiple versions
- Cisco Nexus 9000 Series Fabric Switches – multiple versions
- Cisco UCS Software (UCS Manager Mode) – versions prior to 4.3(6e)
- Cisco UCS Software (Intersight Managed Mode) – versions prior to 4.3(6.260003)

Cisco has indicated that CVE-2026-20127 has been exploited.

Update 1

On February 25, 2026, CISA added CVE-2026-20127 to their Known Exploited Vulnerabilities (KEV) Database.

For more information on these updates, you can follow these URLs:

- Cisco Security Advisories
- Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability
- Cisco Catalyst SD-WAN Vulnerabilities
- Cisco Nexus 3600 and 9500-R Series Switching Platforms Layer 2 Loop Denial of Service Vulnerability
- Cisco Nexus 9000 Series Fabric Switches in ACI Mode SNMP Denial of Service Vulnerability
- Cisco Nexus 9000 Series Fabric Switches in ACI Mode Denial of Service Vulnerability
- Cisco NX-OS Software Link Layer Discovery Protocol Denial of Service Vulnerability
- CISA KEV : CVE-2026-20127

The Guyana National CIRT recommends that users and administrators review these updates and apply them where necessary.

References

- Cisco Security Advisory. (February 25, 2026). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/amd-security-advisory-av26-169

- Cisco Security Advisories. (n.d.). Retrieved from Cisco. https://www.amd.com/en/resources/product-security.html