Exploitation of Cisco SD-WAN appliances

Introduction

Malicious cyber threat actors are targeting Software-Defined Wide Area Networks (SD-WANs) of organizations globally. These actors exploited a Cisco Catalyst SD-WAN controller authentication bypass vulnerability, CVE-2026-20127. After exploitation of this vulnerability the malicious actors add a rogue peer, and eventually gain root access to establish long-term persistence in SD-WANs.

The following agencies, hereafter referred to as the authoring organizations, released a Cisco SD-WAN Threat Hunt Guide, based on investigative data, to support network defenders' detection of and response to the malicious actors' threat activity.

The Hunt Guide is being released by the following authoring and co-sealing agencies:

- United States National Security Agency (NSA)
- United States Cybersecurity and Infrastructure Security Agency (CISA)
- Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)
- Canadian Centre for Cyber Security (Cyber Centre)
- New Zealand National Cyber Security Centre (NCSC-NZ)
- United Kingdom National Cyber Security Centre (NCSC-UK)

Mitigations

The authoring organizations strongly urge network defenders to:

- Collect artifacts, including virtual snapshots and logs off of SD-WAN technology;
- Review Cisco's advisories, Cisco Catalyst SD-WAN Vulnerabilities and Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability, and fully patch SD-WAN technology, including for CVE-2026-20127;
- Hunt for evidence of compromise as detailed in the Hunt Guide; and
- Implement the Cisco Catalyst SD-WAN Hardening Guide.

Cisco's Catalyst SD-WAN hardening guidance should be reviewed in full and includes advice on the following:

- **Network perimeter controls**: Ensure control components are behind a firewall, isolate VPN 512 interfaces, and use IP blocks for manually provisioned edge IPs.

- **SD-WAN manager access**: Replace the self-signed certificate for the web user interface
- **Control and data plane security**: Use pairwise keying Session timeout: Limit to the shortest period possible
- **Logging**: Forward to a remote syslog server

References

- Cisco's Cisco Catalyst SD-WAN Hardening Guide
- ASD's ACSC's Cisco SD-WAN Threat Hunt Guide co-sealed by NSA, CISA, Cyber Centre, NCSC-NZ, and NCSC-UK
- Cisco Talos blog: "Active exploitation of Cisco Catalyst SD-WAN by UAT-8616"
- Cisco security advisory for CVE-2026-20127
- Cisco security advisory for CVE-2026-20122, CVE-2026-20126 and CVE-2026-20128
- See also:
  - CVE-2026-20127
  - CVE-2026-20122
  - CVE-2026-20126
  - CVE-2026-20128

Notices and contact information

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of the authoring organizations' cybersecurity missions, including their responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact information

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov