Critical Cisco SD-WAN Flaw Lets Remote Attackers Take Control

TL;DR

CVE-2026-20127 (CVSS 10) is a maximum-severity authentication bypass vulnerability in Cisco Catalyst SD-WAN Controller and Manager. An unauthenticated remote attacker can gain high-privilege access and manipulate SD-WAN fabric configurations.

Limited exploitation has been observed. There are no workarounds.

Overview

There is a maximum-severity authentication bypass vulnerability (CVE-2026-20127, CVSS 10) affecting Cisco Catalyst SD-WAN Controller (formerly vSmart) and Cisco Catalyst SD-WAN Manager (formerly vManage).

Affected Products

- Cisco Catalyst SD-WAN Controller
- Cisco Catalyst SD-WAN Manager

Deployment types impacted:

- On-Prem Deployment
- Cisco Hosted SD-WAN Cloud
- Cisco Hosted SD-WAN Cloud – Cisco Managed
- Cisco Hosted SD-WAN Cloud – FedRAMP

Organizations should review their deployed version against Cisco's fixed release guidance.

The vulnerability is in the peering authentication process. Due to improper validation, a remote attacker can send crafted requests to a vulnerable control component and successfully log in as an internal, high-privileged account without valid credentials. Once authenticated, the attacker can access NETCONF and modify SD-WAN fabric configurations, including routing and policy settings.

This directly impacts the control plane of the SD-WAN environment. An attacker could alter traffic flows, disrupt connectivity, or manipulate network behavior across sites. Cisco has confirmed limited exploitation in the wild. Due to no workarounds, Aspire recommends patching immediately.

Aspire Protects

- **Patch** - Upgrade immediately to a fixed software release. See Cisco's advisory for patch guidance.
- Restrict ports 22 and 830 to known controller IP addresses only
- Remove unnecessary internet exposure to control components
- Audit authentication and peering logs for suspicious activity

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker sends crafted requests to the exposed SD-WAN control component to exploit the authentication flaw.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker abuses the vulnerability to gain elevated administrative privileges without valid credentials.

Impact

- Modify System Configuration [T1601] – The attacker can alter SD-WAN routing and policy configurations through NETCONF access after gaining control.

Behavioral IoCs

Organizations should review:

Authentication Logs

- /var/log/auth.log
- Look for:
  Accepted publickey for vmanage-admin from <unknown IP>

Note - Any successful login from an unfamiliar IP address should be treated as suspicious.

Peering Events

- Unexpected vmanage peering connections
- Unknown public IP addresses
- Events outside maintenance windows
- Device types inconsistent with deployment architecture

Note - Unauthorized peer connections may appear normal at first glance. Validation is required.

Targeted Industries

This vulnerability threatens any organization using Cisco Catalyst SD-WAN to manage multi-site network connectivity.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire 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

Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability