UPDATE - Cisco SD-WAN Vulnerabilities Allow Authentication Bypass and Unauthorized Access

Author: Portia S. Cole – CTI Researcher

TL;DR

Cisco released patches for multiple Cisco Catalyst SD-WAN vulnerabilities, including CVE-2026-20182 (CVSS 10), which allows an unauthenticated remote attacker to bypass authentication and gain administrative access to affected systems.

Additional vulnerabilities include CVE-2026-20224 (CVSS 8.6), which allows arbitrary file reads, and two privilege escalation flaws, CVE-2026-20209 and CVE-2026-20210 (CVSS 5.4).

Update 5/29/2026

Cisco updated its advisory for CVE-2026-20182 (CVSS 10), the authentication bypass vulnerability affecting Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Manager. The vulnerability and available fixes have not changed. The update adds new guidance to help organizations determine whether a system was compromised before patching.

New Detection Guidance

- Review `/var/log/auth.log` for unauthorized `vmanage-admin` logins.
- Validate SD-WAN peering activity for unexpected or unauthorized connections.
- Review control connection logs for `challenge-ack: 0 entries` that may warrant further investigation.

Example Log Entry

- Accepted publickey for `vmanage-admin` from `[UNKNOWN-IP]`

Updated Recommendations

- Collect admin-tech files before upgrading to preserve potential forensic evidence.
- Retain logs before patching and review them for signs of unauthorized access.
- Review authentication logs for unexpected `vmanage-admin` logins.
- Review SD-WAN peering activity for unauthorized connections.
- See Cisco's updated advisory for more details.

Overview

Cisco disclosed a critical authentication bypass vulnerability in Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Manager tracked as CVE-2026-20182 (CVSS 10). The vulnerability affects multiple SD-WAN deployment models, including on-premises, cloud-managed, and FedRAMP environments.

Cisco said the vulnerability is tied to how SD-WAN control connections verify peer authentication. An attacker can send crafted requests to bypass authentication and gain high-level access to the SD-WAN environment. Cisco confirmed limited exploitation in May 2026.

If exploited, the attacker may gain access to NETCONF services and change SD-WAN configurations across the environment. This could lead to traffic redirection, network outages, unauthorized access, or continued access to the network.

Affected Products

The vulnerabilities affect:

- Cisco Catalyst SD-WAN Controller
- Cisco Catalyst SD-WAN Manager (formerly vManage)

Affected deployment types include:

- On-Prem Deployment
- Cisco SD-WAN Cloud-Pro
- Cisco SD-WAN Cloud (Cisco Managed)
- Cisco SD-WAN for Government (FedRAMP)

Cisco also issued patches for three additional vulnerabilities impacting Cisco Catalyst SD-WAN Manager:

- CVE-2026-20224 (CVSS 8.6) – An unauthenticated XML External Entity (XXE) injection vulnerability that allows remote attackers to read arbitrary files stored on the system through crafted XML requests.

- CVE-2026-20209 (CVSS 5.4) – A privilege escalation vulnerability caused by sensitive session information being recorded in audit logs.

- CVE-2026-20210 (CVSS 5.4) – A privilege escalation vulnerability caused by sensitive information not being properly redacted within configurations and templates.

Cisco stated there is currently no public evidence that CVE-2026-20224, CVE-2026-20209, or CVE-2026-20210 have been exploited. However, many Cisco SD-WAN environments are exposed to the internet, which may increase the risk of future exploitation if systems remain unpatched.

Aspire Protects

- **Patch** - Cisco stated there are no workarounds available for CVE-2026-20182. Customers are advised to collect admin-tech logs before upgrading to preserve potential indicators of compromise.
    - See Cisco's Advisory for more information.
    - Collect admin-tech logs before patching systems impacted by CVE-2026-20182 to preserve potential forensic evidence.
    - Audit /var/log/auth.log for unauthorized vmanage-admin logins related to CVE-2026-20182.
    - Review SD-WAN peering events and show control connections detail output for suspicious activity tied to CVE-2026-20182.
- Restrict internet exposure to SD-WAN management interfaces impacted by CVE-2026-20224.
    - Disable unnecessary services such as HTTP and FTP on systems impacted by CVE-2026-20224.
- Monitor audit logs and configuration changes for suspicious privilege escalation activity associated with CVE-2026-20209 and CVE-2026-20210.
    - See Cisco's advisory for more information regarding CVE-2026-20224, CVE-2026-20209, and CVE-2026-20210.
- Place SD-WAN control components behind firewalls and filtering devices to reduce exposure to CVE-2026-20182 and CVE-2026-20224.
- Open a Cisco TAC case immediately if indicators of compromise related to CVE-2026-20182 are identified.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit exposed Cisco SD-WAN management interfaces to bypass authentication or abuse vulnerable web functionality. (CVE-2026-20182, CVE-2026-20224)

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may abuse vulnerable privilege handling mechanisms to elevate access from low-privileged accounts to administrative access. (CVE-2026-20209, CVE-2026-20210)

Credential Access

- Steal or Forge Authentication Certificates [T1649] – The attacker may abuse the SD-WAN peering authentication process to gain unauthorized trusted access within the SD-WAN environment. (CVE-2026-20182)

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 that use Cisco SD-WAN to connect offices, remote sites, cloud environments, and data centers may be impacted by these vulnerabilities.

- 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

Cisco Catalyst SD-WAN Manager Vulnerabilities