

Actively Exploited Cisco Catalyst SD-WAN Zero-Day Allows Admin Access

Author: Portia S. Cole – CTI Researcher

Overview

Cisco released security updates for CVE-2026-76504 (CVSS 9.8), an authentication bypass vulnerability in Catalyst SD-WAN Manager, formerly known as SD-WAN vManage. The vulnerability affects the API session-based authentication process and can be exploited remotely without credentials.

The vulnerability is caused by improper handling of URI encoding in HTTP requests. An attacker can send a specially crafted request to bypass an authentication rule protecting an API endpoint. Successful exploitation provides access to the API with administrator privileges.

Affected Products

- Cisco Catalyst SD-WAN Manager releases earlier than 20.9
- Cisco Catalyst SD-WAN Manager 20.9
- Cisco Catalyst SD-WAN Manager 20.12
- Cisco Catalyst SD-WAN Manager 20.15
- Cisco Catalyst SD-WAN Manager 20.18
- Cisco Catalyst SD-WAN Manager 26.1
- Cisco Catalyst SD-WAN Manager 26.2

Note: CVE-2026-76504 affects Cisco Catalyst SD-WAN Manager regardless of system configuration. Cisco SD-WAN Cloud has already been updated, and no user action is required for Cisco-managed cloud deployments.

Cisco confirmed that CVE-2026-76504 is being actively exploited. There are no workarounds, and affected systems should be upgraded to a fixed release.

TL;DR

There is a critical vulnerability (CVE-2026-76504, CVSS 9.8) in Cisco Catalyst SD-WAN Manager that allows an unauthenticated remote attacker to bypass authentication and gain administrator access.

Cisco confirmed that the vulnerability is being actively exploited.

Impact on Aspire Customers

If exploited, an attacker could access Cisco Catalyst SD-WAN Manager without a username or password and gain administrator privileges. This could give the attacker access to sensitive information and allow them to make unauthorized changes through the SD-WAN Manager API.

The Common Vulnerability Scoring System (CVSS) rates vulnerabilities from 0 to 10 based on exploitability and potential impact.

- **None** (0.0): No severity
- **Low** (0.1–3.9): Limited impact
- **Medium** (4.0–6.9): Moderate risk
- **High** (7.0–8.9): Serious impact
- **Critical** (9.0–10.0): Severe impact requiring urgent attention

Aspire Protects

- **Patch** - Upgrade Cisco Catalyst SD-WAN Manager to the fixed release. See Cisco's [security advisory](#) for more information.
- Review `serviceproxy-access.log` for `j_security_check` requests from unknown or unauthorized IP addresses.
- Review `vmanage-server.log` for `j_security_check` activity involving usernames beginning with `viptela-reserved-`
- Restrict access to on-premises Catalyst SD-WAN Manager systems from unsecured networks. If internet access is required, limit access to known, trusted hosts.

TTPs to Watch

Initial Access

- **Exploit Public-Facing Application [T1190]**: Attackers can send a crafted HTTP request to the Catalyst SD-WAN Manager API to bypass authentication and access the system with administrator privileges.

IoCs

Cisco recommends checking system logs for signs of exploitation. Requests containing `%6a_security_check` or other encoded characters may indicate suspicious activity and should be reviewed.

Log files to review

- `/var/log/nms/containers/service-proxy/serviceproxy-access.log`
- `/var/log/nms/vmanage-server.log`

Activity to investigate

- `j_security_check` requests from unknown or unauthorized IP addresses
- Requests containing `/%6a_security_check`
- `j_security_check` activity involving usernames beginning with `viptela-reserved-`

Targeted Industries

This vulnerability impacts organizations across industries that use Cisco Catalyst SD-WAN Manager to manage their SD-WAN environments.

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

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's 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.

- **NOC Services Notice**

- If you are an Aspire NOC customer and are affected by any vulnerability in this notice, Aspire will open a case on your behalf. Customers interested in NOC services should contact Aspire's Customer Success Management team.

Supporting Documentation

[Cisco Catalyst SD-WAN Manager API Authentication Bypass Vulnerability NVD-CVE-2026-76504](#)