



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Wednesday, September 30, 2026

CAL-CSIC-202609-A-014

API Authentication Bypass Vulnerability Impacting Cisco Catalyst SD-WAN Manager

Remote Code Execution

Data Exfiltration

IOCs Published

Fixed Releases Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critically-rated vulnerability under active exploitation found in the API session-based management function within Cisco Catalyst SD-WAN Manager. API Session management is the mechanism that maintains the authentication state between a client and the Cisco SD-WAN Manager API and ensures that each API request is tied to a valid, active session to prevent unauthorized access and ensure compliance with security policies.¹ The vulnerability, CVE-2026-76504, carries a CVSS 4.0 score of 9.8.²

CVE-2026-76504 stems from an improper handling of URI coding in an HTTP request, which allows the request to bypass an authentication rule that is intended to restrict access to a specific API endpoint. The vulnerability could allow an unauthenticated, remote attacker to access a vulnerable system with admin privileges. Successful exploitation allows an attacker to obtain a session token with full admin rights to modify configurations, extract data, and disrupt vulnerable networks.³

Cisco has acknowledged the exploit and has issued a security advisory with software updates to address this vulnerability. Additionally, Cisco has published indicators of compromise (IOCs) within their security advisory, and clients are urged to audit their logs and begin hardening their cybersecurity posture. There are no mitigations or workarounds for this exploit.

The Cal-CSIC recommends following Cisco's updating guidance and installing their latest fixed releases as soon as possible.

For additional details regarding CVE-2026-76504, please use this link:

Cisco Security Advisory:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU>

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Affected Products and Versions

Product	Affected Version	Fixed Release
Cisco Catalyst SD-WAN	20.9 and earlier	Migrate to any fixed release
	20.9	20.9.10.1
	20.12	20.12.8.2
	20.15	20.15.6.1
	20.18	20.18.4.1
	26.1	26.1.2.1
	26.2	26.2.1

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

References

¹ Cisco DevNet; "API Reference"; <https://developer.cisco.com/docs/sdwan/overview/#api-reference>; accessed 30 September 2026

² OpenCVE; "CVE-2026-76504"; <https://app.opencve.io/cve/CVE-2026-76504>; accessed 30 September 2026

³ Cisco; "Cisco Catalyst SD-WAN Manager API Authentication Bypass Vulnerability"; <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU>; accessed 30 September 30, 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR