



An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2610010256

NCSC Advisory

Critical vulnerability in Cisco Catalyst SD-WAN Manager

CVE-2026-76504

1st, October 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>. Please treat this document in accordance with the TLP assigned.



Description

CVE ID: CVE-2026-76504

Published: 2026-09-30

Vendor: Cisco

Product: Cisco Catalyst SD-WAN Manager

CVSS Score¹: 9.8

Products Affected

Product	Version
Cisco Catalyst SD-WAN Manager	18.3.6
Cisco Catalyst SD-WAN Manager	18.3.7
Cisco Catalyst SD-WAN Manager	18.3.8
Cisco Catalyst SD-WAN Manager	17.2.10
Cisco Catalyst SD-WAN Manager	18.3.6.1
Cisco Catalyst SD-WAN Manager	18.2.0
Cisco Catalyst SD-WAN Manager	18.4.3
Cisco Catalyst SD-WAN Manager	18.4.1
Cisco Catalyst SD-WAN Manager	17.2.8
Cisco Catalyst SD-WAN Manager	18.3.3.1
Cisco Catalyst SD-WAN Manager	18.4.0
Cisco Catalyst SD-WAN Manager	18.3.1
Cisco Catalyst SD-WAN Manager	17.2.6
Cisco Catalyst SD-WAN Manager	17.2.9
Cisco Catalyst SD-WAN Manager	18.3.4
Cisco Catalyst SD-WAN Manager	17.2.5
Cisco Catalyst SD-WAN Manager	18.3.1.1

¹ <https://www.first.org/cvss/>





Cisco Catalyst SD-WAN Manager	18.3.5
Cisco Catalyst SD-WAN Manager	18.4.0.1
Cisco Catalyst SD-WAN Manager	18.3.3
Cisco Catalyst SD-WAN Manager	17.2.7
Cisco Catalyst SD-WAN Manager	17.2.4
Cisco Catalyst SD-WAN Manager	18.3.0

Impact

A vulnerability in the API session-based authentication management of Cisco Catalyst SD-WAN Manager could allow an unauthenticated, remote attacker to access an affected system with privileges of the admin user.

This vulnerability is due to improper handling of URI encoding in an HTTP request, which allows the request to bypass an authentication rule that is intended to restrict access to a specific API endpoint. An attacker could exploit this vulnerability by sending a crafted HTTP request to the API of the affected system. A successful exploit could allow the attacker to bypass authentication and gain access to the API as the admin user.

Common Weakness Enumeration (CWE)²: CWE-177: Improper Handling of URL Encoding (Hex Encoding)

Known Exploited Vulnerability (KEV) catalog³: Yes

Used by Ransomware Operators: N/A

² <https://cwe.mitre.org>

³ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Cisco.

- <https://nvd.nist.gov/vuln/detail/CVE-2026-76504>
- <https://www.cve.org/CVERecord?id=CVE-2026-76504>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU>
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-76504

