

Critical Vulnerability in Cisco Catalyst SD-WAN Manager Enables Unauthenticated Admin Access



A hex encoding vulnerability in Cisco Catalyst SD-WAN Manager allows unauthenticated remote attackers to gain admin privileges through improper URI encoding handling in HTTP requests.

- CVE-2026-76504 affects Cisco Catalyst SD-WAN Manager with a critical hex encoding flaw
- Unauthenticated remote attackers can exploit improper URI encoding to gain admin-level privileges
- Vulnerability stems from improper handling of URI encoding in HTTP requests
- Organizations must apply vendor mitigations immediately or discontinue product use if patches unavailable
- Internet-exposed SD-WAN management interfaces face elevated risk

Vulnerability Overview

Cisco has disclosed a critical vulnerability tracked as **CVE-2026-76504** affecting Cisco Catalyst SD-WAN Manager. The flaw resides in the system's handling of hex encoding within HTTP requests, specifically in how URI encoding is processed. An unauthenticated, remote attacker can exploit this weakness to access the affected system with full administrative privileges, bypassing normal authentication mechanisms entirely.

The vulnerability's severity stems from its combination of remote exploitability, lack of authentication requirements, and the elevated privileges gained upon successful exploitation. Organizations running SD-WAN infrastructure with management interfaces exposed to the internet face immediate risk.

Risk to Saudi Institutions

Regulated institutions in the Kingdom operating Cisco Catalyst SD-WAN Manager should treat this as a priority incident. The ability for attackers to gain admin-level access without credentials creates exposure to data exfiltration, network manipulation, and potential compliance violations under frameworks including NCA controls and SAMA cybersecurity requirements.

SD-WAN management platforms typically have visibility and control over wide-area network traffic, making compromise particularly consequential for financial institutions, healthcare providers, and critical infrastructure operators.

Immediate Response

Vendor mitigations should be applied immediately in accordance with Cisco's security advisories.

Organizations must inventory all Cisco Catalyst SD-WAN Manager deployments, assess internet exposure of management interfaces, and prioritize patching based on risk. If vendor patches are not yet available, consider network segmentation, access restrictions, or temporary service discontinuation until mitigations can be deployed. Document all actions for audit and compliance purposes.

What to do now

1. Immediately inventory all Cisco Catalyst SD-WAN Manager deployments across your organization
2. Apply vendor-supplied security patches and mitigations as soon as they become available
3. Assess and document internet exposure of all SD-WAN management interfaces
4. Implement network segmentation and access controls to restrict management interface access to trusted networks only
5. If patches are unavailable, consider temporarily discontinuing use or isolating affected systems until mitigations can be deployed
6. Document all remediation actions and timeline for NCA, SAMA or other regulatory compliance reporting