



Cisco SD-WAN Live Protect Shield Release Notes



Cisco SD-WAN Live Protect Shield Release Notes 3

 Vulnerability Overview..... 3

 Affected Releases and Shield Mapping 3

 Known Limitations and Side Effects..... 3

 Recommendations and Deployment 3

 Additional Documentation..... 3

 Disclaimer..... 4

Cisco SD-WAN Live Protect Shield Release Notes

Vulnerability Overview

Live Protect Shield ID: 1000101-01

CVE-ID: CVE-2026-76504

Cisco Security Advisory ID: cisco-sa-sdwan-webauth-xr8beuuJ

A vulnerability in the API session-based authentication management of Cisco Catalyst SD-WAN Manager may allow an unauthenticated, remote attacker to gain unauthorized access to an affected system with administrative privileges. This security flaw is caused by improper handling of URI encoding within HTTP requests, which permits an attacker to bypass authentication rules designed to restrict access to sensitive API endpoints.

Affected Releases and Shield Mapping

The following table outlines the available Live Protect Shields for the affected Catalyst SD-WAN Manager software versions:

Catalyst SD-WAN Release	Live Protect Shield File
20.15 and earlier	Not Available
20.18.3	sdwan-20.18.3-cve-2026-76504-v01.tar.gz
20.18.3.1	sdwan-20.18.3.1-cve-2026-76504-v01.tar.gz
20.18.4	sdwan-20.18.4-cve-2026-76504-v01.tar.gz
26.1.2	sdwan-26.1.2-cve-2026-76504-v01.tar.gz

Known Limitations and Side Effects

Before applying this shield, please be aware of the following potential impact:

Authentication Impact: Legitimate users employing specific URI encoding in their requests may experience intermittent issues when attempting to log into the SD-WAN Manager.

Recommendations and Deployment

While this Live Protect Shield effectively mitigates the primary methods of exploitation, Cisco strongly recommends you upgrade to a software release containing the permanent fix for this vulnerability to ensure full system integrity and coverage.

Deployment Workflow

You can identify and apply available Live Protect Shields directly through the Catalyst Manager Dashboard using **Monitor > Advisories**.

Additional Documentation

For detailed instructions on deploying and managing Cisco Live Protect in your environment, please refer to the [Cisco Catalyst SD-WAN Network Monitoring Guide](#), specifically the chapter, [Secure Cisco Catalyst SD-WAN with Live Protect](#).

Disclaimer

Please be aware that Cisco Vulnerability Shields and Hardening Controls may not fully address potential risks during the device boot process, where systems may remain temporarily exposed before security policies are initialized, nor do they address the risk of system instability should an incompatible Vulnerability Shield cause a boot loop.

Additionally, while Cisco uses commercially reasonable efforts to create effective security technologies, Cisco does not represent or warrant that the Cisco Offer will guarantee absolute security or protect all files, systems, networks, or endpoints from all malwares, malicious attacks, or other threats.

© 2026 Cisco and/or its affiliates. All rights reserved.