



# Cisco Catalyst SD-WAN Manager Reflected HTML Injection Vulnerability



**Advisory ID:**  
cisco-sa-vmanage-html-inj-GxVtK6zj

**First Published:**  
2025 May 7 16:00 GMT

**Version 1.0:** [Final](#)

**Workarounds:** No workarounds available

**Cisco Bug IDs:**  
[CSCwk90639](#)

CVE-2025-20216

CWE-74

**CVSS Score:**  
[Base 4.7](#)

[Download CSAF](#)

[Email](#)

## ^ Summary

A vulnerability in the web interface of Cisco Catalyst SD-WAN Manager, formerly Cisco SD-WAN vManage, could allow an unauthenticated, remote attacker to inject HTML into the browser of an authenticated user.

This vulnerability is due to improper sanitization of input to the web interface. An attacker could exploit this vulnerability by convincing an authenticated user to click a malicious link. A successful exploit could allow the attacker to inject HTML into the browser of an authenticated Cisco Catalyst SD-WAN Manager user.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-html-inj-GxVtK6zj>

## ^ Affected Products

### Vulnerable Products

At the time of publication, this vulnerability affected Cisco Catalyst SD-WAN Manager.

For information about which Cisco software releases were vulnerable at the time of publication, see the [Fixed Software](#) section of this advisory. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

### Products Confirmed Not Vulnerable

Only products listed in the [Vulnerable Products](#) section of this advisory are known to be affected by this vulnerability.

## ^ Workarounds

There are no workarounds that address this vulnerability.

## ^ Fixed Software

When [considering software upgrades](#), customers are advised to regularly consult the advisories for Cisco products, which are available from the [Cisco Security Advisories page](#), to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

## Fixed Releases

This advisory is part of a collection of advisories that describe vulnerabilities in Cisco Catalyst SD-WAN Manager. The collection includes the following advisories:

- [Cisco Catalyst SD-WAN Manager Privilege Escalation Vulnerability](#)
- [Cisco Catalyst SD-WAN Manager Arbitrary File Creation Vulnerability](#)
- [Cisco Catalyst SD-WAN Manager Certificate Validation Vulnerability](#)

- [Cisco Catalyst SD-WAN Manager Arbitrary File Overwrite Vulnerability](#).
- [Cisco Catalyst SD-WAN Manager Stored Cross-Site Scripting Vulnerability](#).
- [Cisco Catalyst SD-WAN Manager Reflected HTML Injection Vulnerability](#).

At the time of publication, the release information in the following table was accurate. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

In the following table, the left column lists Cisco software releases. The center column indicates whether a release is affected by the vulnerability described in this advisory and the first release that includes the fix for this vulnerability. The right column indicates whether a release is affected by any of the vulnerabilities that are part of this collection of advisories and which release includes fixes for all vulnerabilities in this collection.

Customers are advised to upgrade to an appropriate fixed software release.

Cisco Catalyst SD-WAN Manager Release	First Fixed Release for This Vulnerability	First Fixed Release for All Vulnerabilities in This Collection
20.8 and earlier <sup>1</sup>	Migrate to a fixed release.	Migrate to a fixed release.
20.9 <sup>2</sup>	20.9.7	Migrate to a fixed release.
20.10 <sup>1</sup>	Migrate to a fixed release.	Migrate to a fixed release.
20.11 <sup>1</sup>	Migrate to a fixed release.	Migrate to a fixed release.
20.12	20.12.5	Migrate to a fixed release.
20.13 <sup>1</sup>	Migrate to a fixed release.	Migrate to a fixed release.
20.14 <sup>2</sup>	Migrate to a fixed release.	Migrate to a fixed release.
20.15	20.15.2	Migrate to a fixed release.
20.16	Not vulnerable.	20.16.1

1. These releases have reached [End of Software Maintenance](#). Cisco strongly encourages customers to [upgrade to a supported release](#).
2. These releases have entered the end-of-life process. For milestone dates for a specific release, see the [End-of-Sale and End-of-Life Announcement](#) for that release.

When considering a software migration, customers are advised to regularly consult the advisories for Cisco products, which are available from the [Cisco Security Advisories page](#), to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the new software will be sufficient for their network needs and that current hardware and software configurations will continue to be supported properly by the new product. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

## ⤴ Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

## ⤴ Source

Cisco would like to thank the external researcher who reported this vulnerability.

## ⤴ URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-html-inj-GxVtK6zj>

## ⤴ Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2025-MAY-07

## ⤴ Legal Disclaimer

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

▶ Cisco Security Vulnerability Policy

▶ Subscribe to Cisco Security Notifications

▶ Related to This Advisory

Your Rating:



Average Rating:



5 star	0
4 star	0
3 star	0
2 star	0
1 star	0

[Leave additional feedback](#)

Quick Links

- About Cisco
- Contact Us
- Careers
- Connect with a partner

Resources and Legal

- Feedback
- Help
- Terms & Conditions
- Privacy
- Cookies / Do not sell or share my personal data
- Accessibility
- Trademarks
- Supply Chain Transparency
- Newsroom
- Sitemap

