Remediate Catalyst SD-WAN Security Advisory - September 2026

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Remediation Workflow Overview

Step 1: Collect Admin-Tech Files from All Managers

- Alternative: Manual Verification (Only if Admin-Tech Cannot Be Collected)

Step 2: Upgrade to a Fixed Software Version

Step 3: Open a TAC Case and Upload Admin-Tech Files for Scanning

Step 4: If Compromise is Identified — TAC Guidance

Fixed Software Versions

- Important References

Appendix: Manual Verification Steps (Only if Admin-Tech Collection is Not Possible)

- How to Identify the Indicators of Compromise
- Verification 1: Audit the Service Proxy Access Log
- Verification 2: Audit the Manager Server Log

Frequently Asked Questions

Introduction

This document describes steps to identify and fix a critical SD-WAN security vulnerability per the PSIRT advisory dates September 30,2026. Cisco strongly recommends upgrading to a fixed software release to remediate this issue.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Catalyst SD-WAN architecture and control components (Manager, Controller and Validator)
- Cisco Catalyst SD-WAN upgrade procedure
- Cisco TAC case management and admin-tech collection procedures

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure

that you understand the potential impact of any command.

Background Information

For detailed background information and the latest updates, refer to the official PSIRT advisory page.

This advisory is available at this link:

- Cisco Catalyst SD-WAN Manager API Authentication Bypass Vulnerability (CVE-2026-76504, CWE-177). Security Impact Rating: Critical (CVSS Base Score 9.8).

This defect is addressed by this PSIRT advisory:

- Cisco bug ID CSCww79570

This advisory affects Cisco Catalyst SD-WAN Manager (vManage).

Remediation Workflow Overview



Note: All SD-WAN Managers (vManage) that run a release earlier than the first fixed release are vulnerable and require an immediate upgrade. However, not all Catalyst Managers show evidence of compromise.

Required Action: Collect admin-techs from all Catalyst SD-WAN Managers, upgrade all to a fixed release, and open a Cisco TAC case so TAC can scan your admin-techs for indicators of compromise.

TAC is available to:

- Scan the admin-techs you provide for indicators of compromise
- Provide upgrade support if you encounter issues during the upgrade
- Guide you through additional remediation if indicators of compromise are identified

1. **Collect Admin-Techs** - Run admin-tech on all Catalyst SD-WAN Managers, including every node of a cluster and of a Disaster Recovery (DR) deployment, **prior to the upgrade to ensure no diagnostic data is lost.** Select Log and Tech options. Core is not required.
2. **Upgrade to a Fixed Release** - Upgrade all Managers (vManage) to a fixed software version listed in the Fixed Software Versions table. Do not wait for TAC scan results before upgrading. Upgrading to a fixed release is the highest priority and closes the vulnerability. The TAC scan in Step 3 determines whether any further action is needed after the upgrade.
3. **Open a TAC Case and Upload Admin-Techs to scan for indicators of compromise** - Open a Cisco TAC case and upload all admin-tech log bundles collected in Step 1. TAC scans the admin-techs for indicators of compromise.
4. **If Compromise is Identified, use the TAC Guidance** - If TAC identifies indicators of compromise in your environment, complete all remediation guidance provided by TAC. If no indicators of compromise are found, no further action beyond the upgrade is required.

Step 1: Collect Admin-Tech Files from All Managers

Required: Collect admin-tech files from all Managers (vManage) before upgrading to ensure no diagnostic data is lost. These files are used by TAC in Step 3 to scan your environment for indicators of compromise.

Collection:

For admin-tech generation, select Log and Tech options. Core is not required.

1. Run admin-tech on **ALL Managers** (vManage).
2. If your Managers run as a cluster, run admin-tech on **every cluster member**.
3. If you have a Disaster Recovery (DR) deployment, run admin-tech on **every Manager in both the primary and the DR site**.

Collect an Admin-Tech in SD-WAN Environment and Upload to TAC Case

TAC analyzes these files to assess your environment for indicators of compromise and guide the appropriate remediation path.

Alternative: Manual Verification (Only if Admin-Tech Cannot Be Collected)

For those who cannot share admin-tech files, manual verification steps are available. These steps provide preliminary indicators that must be documented and shared with TAC.

See the Manual Verification Steps section at the end of this document for detailed procedures. Document all findings and provide them to TAC in your support case.

Step 2: Upgrade to a Fixed Software Version

After collecting admin-techs in Step 1, upgrade all Managers (vManage) to a fixed software version.



Important: Do not wait for TAC scan results before upgrading. Upgrading to a fixed release is the highest priority and closes the vulnerability. The TAC scan in Step 3 determines whether any further action is needed *after* the upgrade.

Select the appropriate version from the Fixed Software Versions table in this document.



Warning: **Upgrade must remain within your current major release.** Do not upgrade to a higher major release without explicit TAC guidance.

Upgrade SD-WAN Controllers with the Use of vManage GUI or CLI

If you encounter any issues during the upgrade, open a TAC case for upgrade support.

Step 3: Open a TAC Case and Upload Admin-Tech Files for Scanning

After upgrading in Step 2, **open a Cisco TAC support case** and upload the admin-tech files collected in Step 1. TAC scans the admin-techs for indicators of compromise.

Required Actions:

1. Open a Severity 3 TAC case with the CVE-ID "**CVE-2026-76504**" in the title to initiate the scanning process.
2. Upload ALL admin-tech log bundles collected in Step 1 (all Managers, including cluster and DR nodes).
3. Wait for TAC to complete the scan and communicate the results.

TAC analyzes the admin-tech files and communicates the results of the scan. If no indicators of compromise are found, no further action beyond the upgrade is required.

Step 4: If Compromise is Identified — TAC Guidance

If TAC identifies indicators of compromise in your environment, TAC contacts you with specific remediation guidance. Complete all instructions provided by TAC.

If no indicators of compromise are identified, the upgrade completed in Step 2 is sufficient and no further remediation is required.

Fixed Software Versions

These software releases contain the fix for this vulnerability. Upgrade to the first fixed release in your current release train.

Cisco Catalyst SD-WAN Software Release	First Fixed Release	Available Software
Earlier than 20.9[1]	Migrate to a fixed release.	
20.9	20.9.10.1	20.9.10.1 upgrade images for vManage
20.12	20.12.8.2	20.12.8.2 upgrade images for vManage
20.15	20.15.6.1	20.15.6.1 upgrade images for vManage
20.18	20.18.4.1	20.18.4.1 upgrade images for vManage
26.1	26.1.2.1	26.1.2.1 upgrade images for vManage
26.2	26.2.1	26.2.1 upgrade images for vManage

[1] These releases have reached End of Software Maintenance. Cisco strongly encourages customers to upgrade to a supported release.

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

Cisco has also addressed this vulnerability in Cisco SD-WAN Cloud (Cisco Managed) Release 20.15.605, which is cloud based. No user action is required. Customers can determine the current remediation status or software version by using the Help function in the service GUI.

Important References

- Upgrade Matrix
- Controller Compatibility Matrix

Appendix: Manual Verification Steps (Only if Admin-Tech Collection is Not Possible)

Admin-tech collection is the preferred and recommended method. Only use manual verification if you absolutely cannot collect and share admin-tech files. If you cannot collect admin-tech files, use these manual steps to gather preliminary indicators for TAC.

- These steps provide preliminary data only
- Admin-tech collection is strongly preferred for accurate assessment
- Document your findings and share them with TAC in your support case
- TAC makes the official assessment determination

Requirements: These steps must be performed on all Managers (vManage), including every cluster member and every Manager in a Disaster Recovery (DR) site. Access the log files from vshell (vshell from the Manager CLI), and review both the current and the rotated log files.

How to Identify the Indicators of Compromise

This advisory has two indicators of compromise. Both relate to entries for j_security_check in which a character of the request is encoded (for example /%6a_security_check), from unknown or unauthorized IP addresses.



Important: The examples in this section show the use of %6a as the encoded character j in the request. This is only an example, and the vulnerability allows any one character that is encoded in the request to be used.

Cisco Catalyst SD-WAN Manager systems exposed to the internet and with ports exposed to the internet are at risk of exposure to compromise. In some instances, these indicators of compromise can occur during standard operations. Therefore, they must be assessed against normal network posture to identify and avoid false positives.

Indicator	Log File	What It Means	Verification
Encoded j_security_check request received	/var/log/nms/containers/service_proxy/serviceproxy-access.log*	A client sent a request of this type to the Manager.	Verification 1
Encoded j_security_check request processed for a viptela-reserved-* user	/var/log/nms/vmanage-server.log*	The Manager processed a request of this type for a viptela-reserved-* user (a reserved system service account).	Verification 2

Verification 1: Audit the Service Proxy Access Log

Audit the serviceproxy-access.log file, located at /var/log/nms/containers/service_proxy/serviceproxy-access.log, for entries that are related to j_security_check from unknown or unauthorized IP addresses, as shown in this example:

```
[2026-09-29T23:11:13.948-05:00] "POST /%6a_security_check HTTP/1.1" 200 - 48 0 4 - "10.10.10.47,192.168
```

Certain log files in the vManage system are restricted behind root access and cannot be accessed directly by customers. To review these logs, customers must generate an admin-tech file.

Interpret Results and Document for TAC

If no such entries are found:

- No indicators of compromise detected in this log on this Manager
- Document this result for your TAC case
- Continue with Verification 2, and then repeat both verifications on the remaining Managers

If such entries are found:

- Carefully examine each source IP address shown
- Look for entries from unknown or unauthorized IP addresses. Verify whether the source IP belongs to an authorized activity in your environment (for example, a vulnerability scan or penetration test that you run)
- If you cannot identify the source IP as legitimate, this can indicate potential indicators of compromise
- **Document all findings and open a TAC case immediately**
- Include the log entries, timestamps, source IPs, and HTTP status codes in your case
- TAC performs the official assessment determination

Verification 2: Audit the Manager Server Log

Audit the vmanage-server.log file, located at /var/log/nms/vmanage-server.log, for entries that are related to j_security_check from unknown or unauthorized IP addresses, specifically being called for users that include names starting with viptela-reserved-, as shown here:

```
29-Sep-2026 23:11:13,952 CDT [] [vManage-new] [UserUtils] (default task-127462) |default| Request Store
```

The viptela-reserved system service accounts are documented in the Authentication, Authorization, and Accounting section of the Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide.

Interpret Results and Document for TAC

If no such entries are found:

- No indicators of compromise detected in this log on this Manager
- Document this result for your TAC case
- Repeat both verifications on the remaining Managers

If such entries are found:

- This can indicate potential indicators of compromise
- **Document all findings and open a TAC case immediately**
- Include the log entries and timestamps in your case, together with the Verification 1 findings for the same time period
- TAC performs the official assessment determination

Frequently Asked Questions

What is the first step to address this security advisory?

Collect admin-tech files from all Managers (vManage), then upgrade all Managers to a fixed software version. After upgrading, open a TAC case and upload the admin-techs so TAC can scan your environment for indicators of compromise.

Which components are affected by this advisory?

Only Cisco Catalyst SD-WAN Manager (vManage) is affected.

Do we need to upgrade the Controllers, Validators, or edge routers as well?

No, not to address this advisory. Upgrade all Managers (vManage) to a fixed release, and use the Controller Compatibility Matrix to confirm that the new Manager release is compatible with your other components.

Is a workaround available?

No. There are no workarounds that address this vulnerability. Upgrade to a fixed release.

What version do I need to upgrade to?

Upgrade to the first fixed release in your current release train as soon as possible. Refer to the Fixed Software Versions table in this document. TAC confirms the appropriate version for your specific environment.

I already upgraded to a fixed release for a previous SD-WAN security advisory. Do I need to upgrade again?

Yes, unless your current release is at or later than the first fixed release in your train in the Fixed Software Versions table. Fixed releases for earlier advisories do not necessarily include the fix for this vulnerability.

Do I need to collect admin-techs from all Managers?

Yes. TAC requires admin-tech files from every Manager (vManage), including every cluster member and every Manager in a Disaster Recovery (DR) site, to properly assess your environment.

Can I check for indicators of compromise myself?

Yes. If you cannot collect admin-tech files, use the Manual Verification Steps on every Manager and share the results with TAC. Admin-tech collection remains the preferred method, and TAC makes the official assessment determination.

How does TAC determine if my system has been compromised?

TAC analyzes the admin-tech files using specialized tools to assess your environment for indicators of compromise.

What happens if indicators of compromise are identified?

TAC contacts you to discuss next steps and guidance specific to your environment. Cisco does not perform the remediation on your behalf — TAC provides the guidance needed for you to proceed.

Can I start the upgrade before TAC analyzes my admin-techs?

Yes. Collect admin-techs, upgrade to a fixed release, and then open a TAC case so TAC can scan the admin-techs for indicators of compromise.

Is downtime expected during remediation?

The impact depends on your deployment architecture and the remediation path. TAC provides guidance on minimizing service impact during the process.

I have a cloud-hosted SD-WAN overlay. What are my options for upgrading?

For cloud-hosted overlays, customers have two options:

1. Check if your environment is scheduled for an automated upgrade by navigating to SSP > Overlay Details > Change Windows.
2. If you do not want to wait for the scheduled upgrade, you have two options:
    - Upgrade on your own using the upgrade guides available in this document.
    - Open a standby TAC case for your preferred maintenance window. TAC is available to assist you if you encounter difficulties with the upgrade.

We are a Cisco-hosted overlay. Do we need to review any access rules on SSP?

All Cisco-hosted customers are advised to review their own Allowed Inbound Rules in SSP > Overlay Details > Allow Inbound rules and ensure only the necessary prefixes from your side are allowed. These rules are for management access only and do not apply to edge routers.

Does Cisco TAC provide forensic analysis or investigation services for this vulnerability?

Cisco TAC can assist customers by scanning for Indicators of Compromise (IoCs) related to this vulnerability. However, TAC does not perform in-depth forensic analysis or incident investigations. For comprehensive forensic work or detailed security investigations, we recommend that customers engage their preferred third-party Incident Response (IR) firm.

What are the general best practices or ways to reduce vulnerabilities for my SD-WAN overlay?

Refer to the Cisco Catalyst SD-WAN Hardening Guide for best practices and recommendations to reduce vulnerabilities in your SD-WAN overlay.

Which Controller (vSmart) and Validator (vBond) releases should I run with the Manager (vManage) release that fixes this advisory?

This advisory affects Cisco Catalyst SD-WAN Manager (vManage) only, so only the Manager moves to a new release. Upgrade each Manager to the first fixed release for your train in the Fixed Software Versions table.

Controllers and Validators do not require an upgrade for this advisory: they are expected to already run the fixed release published in the Cisco Catalyst SD-WAN Software Security Hardening Release: August 2026 advisory, and that release in the same train is the expected pairing for the fixed Manager release.

Your release train is the major version family you run today, such as 20.9, 20.12, 20.15, 20.18, 26.1, or 26.2. The first fixed release is the earliest release within that same train that contains the fix, and it is the shortest, lowest-risk path to remediation because you stay in the train you already run. You do not need to move to a newer train to address this advisory. If your Manager is already at or later than the first fixed release for your train, it is not affected and no upgrade is required. Only releases earlier than 20.9 require a migration to a supported train, because those releases have reached End of Software Maintenance.

Use your normal upgrade process and the same maintenance throttle you used for the previous advisory. The

only change is that you select the new Manager image. For example, in the 20.15 train:

- Manager (vManage) — 20.15.6.1
- Controllers (vSmart) and Validators (vBond) — 20.15.6

If your control components are still on a release that predates the August 2026 advisory, follow the standard SD-WAN upgrade order and start with the Manager. For example, if your components are on 20.9.5:

1. Upgrade each Manager (vManage) directly to the release that fixes this advisory, which is 20.9.10.1 in the 20.9 train.
2. Upgrade the Validators (vBond) and Controllers (vSmart) to the August 2026 fixed release for that train, which is 20.9.10.

In this example, the end state is Managers at 20.9.10.1 and Validators and Controllers at 20.9.10. The 20.9 releases are shown only as an example; apply the same sequence to the train you run, using the Fixed Software Versions table to identify the correct Manager release for your train.

Where can I check which Controller (vSmart) and Validator (vBond) versions are compatible with the Manager (vManage) release that contains this fix?

Use the Controller Compatibility Matrix. Look up the Manager release you are upgrading to from the Fixed Software Versions table, and confirm the supported Controller and Validator releases for it. The Upgrade Matrix shows the supported upgrade paths to reach that release.