Remediate Catalyst SD-WAN Security Advisory - Jun 2026

Contents

Introduction

This document describes steps to identify and address critical security vulnerabilities in SD-WAN based on PSIRT advisories dated Jun 4th, 2026.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Catalyst SD-WAN architecture and control components (vManage, vSmart, vBond)
- 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.

These advisories are available at these links:

- Cisco Catalyst SD-WAN Manager Authenticated Privilege Escalation Vulnerability

These defects are addressed by these PSIRT advisories:

- Cisco bug ID CSCwu18563

Remediation Workflow Overview

This advisory describes a privilege-escalation vulnerability in SD-WAN Manager that requires netadmin privileges to exploit.

Per the advisory, the known paths for an unauthenticated remote attacker to obtain those privileges are exploitation of CVE-2026-20182 (cisco-sa-sdwan-rpa2-v69WY2SW) or CVE-2026-20127 (cisco-sa-sdwan-rpa-EHchtZk).

If your control components have been upgraded to a fixed release for both of those advisories, and Cisco did not identify any potential Indicators of Compromise (IoCs) in the admin-tech files you provided for the prior events, then the known unauthenticated exploitation paths for this new vulnerability are mitigated on those specific devices, based on the files reviewed.

This does not eliminate exposure where an attacker holds valid netadmin credentials. Cisco has not yet released a software fix for this vulnerability, and no workarounds are available; further guidance will follow as it becomes available.

Required Action: Open a Cisco TAC case to address this security advisory.

TAC is available to:

- Assess your environment for indicators of compromise
- Guide you through the appropriate remediation path based on the assessment
- Provide guidance on next steps needed to take if indicators of compromise are identified

1. **Collect Admin-Techs**- Run admin-tech on all control components (vSmart, vManage, vBond). vSmart admin-techs must not be run simultaneously — run them one at a time. All others can be collected in any order. Select Log and Tech options. Core is not required.
2. **Open TAC Case**- Contact Cisco TAC and provide all Control Component Admin-tech log bundles.
3. **TAC Assessment**- Perform a preliminary assessment of indicators of compromise within your environment and TAC performs a preliminary assessment of indicators of compromise in your environment.
4. **Execute Remediation**- Complete the specific process provided by TAC if required.

Step 1: Collect Admin-Tech Files from All Control Components

Required: Collect admin-tech files from all control components **before any upgrade or configuration change** so that diagnostic data and any potential indicators of compromise (IoCs) are preserved. These files are used by TAC in Step 3 to analyze your environment.

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

1. Run admin-tech on **ALL Controllers** (vSmarts) — **do not run these simultaneously; collect one at a time**
2. Run admin-tech on **ALL Managers** (vManages)
3. Run admin-tech on **ALL Validators** (vBonds)

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

---

Note: TAC analyzes these files to assess your environment for indicators of compromise related to this advisory. The analysis for this advisory focuses on a specific log entry that does not distinguish between legitimate and malicious use; manual review by TAC is required.

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

For customers who cannot share admin-tech files, a manual verification step is available. This step provides a preliminary indicator that must be documented and shared with TAC.

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

Step 2: Open a TAC Case and Upload Admin-Tech Files

After collecting admin-techs in Step 1, **open a Cisco TAC support case** and upload the admin-tech files collected. TAC analyzes the admin-techs for indicators of compromise associated with this advisory.

Required Actions:

1. Open a Severity 3 TAC case with “CVE-2026-20245” and the advisory ID `cisco-sa-sdwan-privesc-4uxFrdzx` in the title to initiate the analysis.
2. Upload ALL admin-tech log bundles collected in Step 1 (Controllers, Managers, and Validators).
3. Wait for TAC to complete the analysis and communicate the results.

Note: Cisco has not released a software fix for this vulnerability and no workarounds are available. The TAC analysis in Step 3 helps determine whether any indicators of compromise are present in the admin-tech files you provided. Further guidance will follow as it becomes available from engineering.

Step 3: TAC Assessment

TAC performs a preliminary analysis of the admin-tech files you uploaded in Step 2 and assesses them for indicators of compromise associated with this advisory.

For this advisory, the analysis is focused on a specific log entry in `/var/log/scripts.log` on each Manager (vManage). Because the underlying command is legitimate and the log does not distinguish between legitimate and malicious use, any matching entries require manual review by TAC against the customer's normal operational posture before being treated as a confirmed indicator.

Possible outcomes of the TAC analysis:

- **No matching log entries identified** — based on the admin-tech files reviewed, no indicators associated with this advisory were observed. No further action specific to this advisory is required at this time. The result is limited to the admin-tech files received and may be limited by the log retention period on each device.
- **Matching log entries identified** — TAC will engage the customer with additional review steps. Because Cisco has not released a software fix for this advisory, the upgrade alone does not resolve this vulnerability. TAC's guidance for confirmed-compromise scenarios is documented in the related TechZone articles referenced in Step 4.

Note: Per the advisory, exploitation of this vulnerability requires *netadmin* privileges, which an unauthenticated attacker can obtain only through valid credentials or exploitation of CVE-2026-20182 or CVE-2026-20127. If your control components have been upgraded to a fixed release for both of those advisories and no indicators of compromise were identified for the prior events, the known unauthenticated exploitation paths for this new vulnerability are mitigated on those specific devices, based on the files reviewed.

Step 4: If Indicators of Compromise Are Identified — Follow TAC Guidance

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

If no indicators of compromise are identified for this advisory, no further action specific to this advisory is required at this time, based on the admin-tech files reviewed.

Important: Cisco has not released a software fix for this advisory and no workarounds are available. Because exploitation of this vulnerability requires *netadmin* privileges obtained through CVE-2026-20182 or CVE-2026-20127, customers should ensure remedination of those prior advisories is complete. Refer to the corresponding documents for the established remediation flow:

Considerations

At the conclusion of a successful remediation, and based on each customer's specific security assurance requirements, customers may wish to evaluate and act on the following hygiene activities. These activities apply regardless of which remediation option is selected. They are customer-managed; Cisco does not direct or perform them on the customer's behalf.

- Review of all local user accounts

- Rotation of credentials
- Rotation of any secrets present in device configurations, for example (non-exhaustive list):
    - Credentials for local user accounts
    - SNMP community strings
    - TACACS secret keys
    - VPN pre-shared keys and certificates
    - Trusted SSH keys
- Review of configuration templates

Edge Devices — Suspected Compromise

Cisco does not recommend a particular remediation path; the selection of a remediation option rests with the customer. As an informational note for customers evaluating their environment: where compromise of an edge device is suspected by the customer, a factory reset and re-onboarding of the affected edge device(s) is a customer-managed action that the customer may wish to take into account when making their selection. The decision whether to pursue this approach, and which option to select, rests with the customer.

The proper command to perform a secure factory reset is:

```
factory-reset all secure 3-pass
```

Fixed Software Versions

⚠ **Important**: At the time of publication of this document, **Cisco has not released a software fix that addresses CVE-2026-20245**. Per the advisory, Cisco plans to address this vulnerability in Cisco Catalyst SD-WAN Manager in a future release. There are no workarounds. This section will be updated when fixed software becomes available.

Because exploitation of this vulnerability requires *netadmin* privileges that an unauthenticated attacker can obtain only through CVE-2026-20182 or CVE-2026-20127, customers are encouraged to ensure their control components are running a fixed release for those prior advisories. The fixed releases for those advisories are documented in the May 14, 2026 SD-WAN Security Advisory and the corresponding TechZone document:

- Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability (May 14, 2026)
- (Fixed Software Versions table)

Important References:

- Upgrade Matrix
- Controller Compatibility Matrix

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

Note: Admin-tech collection is the preferred method. Only use the manual verification step below if admin-tech files cannot be collected and shared with TAC. The result of this manual step is preliminary; document findings and share them with TAC, who performs the official assessment.

Note: For this advisory, the manual verification consists of a single targeted log check. The log entry searched for is generated by a **legitimate** command and the log alone does not distinguish between legitimate and malicious use. Any matching entry must be reviewed against the customer's normal operational posture before being treated as a potential indicator. If a matching entry cannot be reconciled with normal operations, document the finding and share it with TAC.

Verification: Check `scripts.log` on each Manager (vManage) for Tenant List Upload Entries

Per the PSIRT advisory, customers are encouraged to audit the `scripts.log` file, located at `/var/log/`, for entries similar to the following example:

```
Apr 15 09:44:57 vmanage vScript: Tenant list upload per vsmart serial number: /usr/bin/vconfd_script_up
```

Step 1: Access vshell on each Manager (vManage) and search the log file

From the vManage CLI, drop into vshell and run:

```
vs
zgrep "vconfd_script_upload_tenant_list.sh" /var/log/scripts.log*
```

Repeat the check on every vManage in the deployment (including all cluster members and any DR-paired vManage).

Step 2: Interpret Results and Document for TAC

If NO matching entries are returned:

- No indicators of compromise associated with this advisory were observed in the log file on this device.
- Document this result for your TAC case (include the device hostname and the date/range of the log files searched).
- Continue the check on the remaining Managers.

If matching entries are returned:

- Each matching entry must be reviewed against the customer's normal operational posture. The underlying command (tenant list upload) is legitimate and may appear during routine operations.
- For each matching entry, capture the timestamp, the full log line, and the file path referenced after -

`cli path`.
- If a matching entry cannot be reconciled with a known, legitimate operation, this may be an indicator of compromise. Document the finding and provide it to TAC for review.
- **Document all findings and open a TAC case**. Include the matching log entries and the source command output in your case.
- TAC performs the official assessment. If the assessment identifies indicators of compromise, follow the flow described in the related TechZone documents: and remediation guides.

Frequently Asked Questions

Q: What is the first step to address this security advisory?

A: Collect admin-tech files from all control components (vSmart, vManage, vBond) before any upgrade or configuration change to preserve diagnostic data and any potential indicators of compromise. Then open a Cisco TAC case and upload the admin-techs so TAC can analyze them.

Q: Has Cisco released a software fix for this vulnerability?

A: Not at the time of publication of this document. Per the advisory, Cisco plans to address this vulnerability in Cisco Catalyst SD-WAN Manager in a future release. There are no workarounds. This document will be updated when a fixed release becomes available.

Q: If there is no fix, why does Cisco recommend any action now?

A: Exploitation of this vulnerability requires *netadmin* privileges. Per the advisory, an unauthenticated attacker can obtain those privileges only through valid credentials or through exploitation of CVE-2026-20182 or CVE-2026-20127. Ensuring control components are upgraded to the fixed releases for those prior advisories addresses the known unauthenticated paths to obtaining the privileges required to exploit this vulnerability. The admin-tech analysis in Step 3 helps determine whether any indicators of compromise are present in the files reviewed.

Q: Do I need to collect admin-techs from all control components?

A: Yes. TAC requires admin-tech files from all Controllers **(vSmart, collected one at a time)**, all Managers (vManage), and all Validators (vBond) to perform the analysis.

Q: How does TAC determine if my system has indicators of compromise associated with this advisory?

A: TAC reviews the admin-tech files and looks for the specific log entry described in the PSIRT advisory in `/var/log/scripts.log` on each Manager. The underlying command is legitimate; any matching entry must be reviewed against your normal operational posture before being treated as a potential indicator. TAC performs that review.

Q: What happens if indicators of compromise are identified?

A: TAC contacts you with specific guidance. Because no software fix is currently available for this advisory, the upgrade alone does not resolve a confirmed compromise. TAC's guidance follows the flow documented in the related TechZone articles for the May 2026 and February 2026 advisories.

Q: Are edge routers (Cisco IOS XE) affected by this advisory?

A: This advisory affects Cisco Catalyst SD-WAN Manager. Per the advisory, Cisco has observed limited cases where exploitation of this vulnerability resulted in a configuration change pushed to edge devices;

customers are encouraged to verify the configuration of their edge devices.

Q: Which deployment types are affected?

A: Per the advisory, this vulnerability affects all Cisco Catalyst SD-WAN Manager deployment types regardless of device configuration, including On-Prem Deployment, Cisco SD-WAN Cloud-Pro, Cisco SD-WAN Cloud (Cisco Managed), and Cisco SD-WAN for Government (FedRAMP).

Q: I have already upgraded for the May 2026 and February 2026 advisories and no indicators of compromise were identified for those events. Am I exposed to this new vulnerability?

A: If your control components are running a fixed release for both CVE-2026-20182 and CVE-2026-20127 and no indicators of compromise were identified for those prior events in the admin-tech files reviewed, the known unauthenticated exploitation paths for this new vulnerability are mitigated on those specific devices, based on the files reviewed. This does not eliminate exposure where an attacker holds valid *netadmin* credentials.

Q: Can I perform the verification myself instead of waiting for TAC?

A: Customers who cannot share admin-techs may perform the manual verification step described in the Appendix. The result is preliminary; document findings and share them with TAC, who performs the official assessment.

Q: What are the general best practices for hardening my SD-WAN overlay?

A: Refer to the Cisco Catalyst SD-WAN Hardening Guide for best practices.

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

A: Cisco TAC can assist customers by reviewing admin-tech files for the indicators of compromise documented in the PSIRT advisory. Cisco TAC does not perform in-depth forensic analysis or incident investigations. For comprehensive forensic work or detailed security investigations, customers are encouraged to engage their preferred third-party Incident Response (IR) firm.