Remediate Catalyst SD-WAN Security Advisory - June 2026

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Remediation Workflow Overview

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

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

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

Step 3: TAC Assessment

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

Fixed Software Versions

Considerations

- Edge Devices — Suspected Compromise

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

- Verification for CVE-2026-20245: Check scripts.log on each control component for File Upload Entries
- Verification for CVE-2026-20262: Check Log Files on each Manager (vManage) for Arbitrary File Write Entries

Frequently Asked Questions

Introduction

This document describes steps to identify and address critical security vulnerabilities in SD-WAN based on PSIRT advisories dated June 4 and 15, 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 Controller, Catalyst SD-WAN Manager, and Catalyst SD-WAN Validator Authenticated Privilege Escalation Vulnerability
- Cisco Catalyst SD-WAN Manager Arbitrary File Write Vulnerability

These defects are addressed by these PSIRT advisories:

- Cisco bug ID CSCwu18563
- Cisco bug ID CSCwu18441

Remediation Workflow Overview

These advisories describe two vulnerabilities in Cisco Catalyst SD-WAN. The first (CVE-2026-20245) is a privilege-escalation vulnerability in SD-WAN control components that requires netadmin privileges to exploit. The second (CVE-2026-20262) is an arbitrary file write vulnerability in SD-WAN Manager (vManage) that allows an authenticated user to create or overwrite any file on the filesystem of an affected system.

For both CVE-2026-20245 and CVE-2026-20262, the known paths for an unauthenticated remote attacker to obtain the required credentials are exploitation of CVE-2026-20182 (cisco-sa-sdwan-rpa2-v69WY2SW) or CVE-2026-20127 (cisco-sa-sdwan-rpa-EHchtZk). CVE-2026-20245 requires netadmin privileges to exploit, while CVE-2026-20262 requires at least a lower-privileged single-task user account.

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 both CVE-2026-20245 and CVE-2026-20262 are mitigated on those specific devices, based on the files reviewed. This does not eliminate exposure where an attacker holds valid credentials. Cisco recommends you upgrade to a fixed release for both advisories.

Required Action: Open a Cisco TAC case to address these security advisories.

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 the next steps 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** - TAC performs a preliminary assessment of indicators of compromise in your environment based on the admin-tech files provided.

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 an SD-WAN Environment and Upload to a TAC Case

---



Note: TAC analyzes these files to assess your environment for indicators of compromise related to both advisories. For the privilege escalation advisory, the analysis focuses on a specific log entry in `/var/log/scripts.log` that does not distinguish between legitimate and malicious use; manual review by TAC is required. For the arbitrary file write advisory, the analysis focuses on entries in `/var/log/nms/vmanage-server.log`; these entries can also occur during standard operations and must be assessed against normal operational posture to avoid false positives.

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

If you 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 a 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 both advisories (CVE-2026-20245 and CVE-2026-20262).

Required Actions:

1. Open a Severity 3 TAC case with “CVE-2026-20245, CVE-2026-20262” and the advisory IDs `cisco-sa-sdwan-privesc-4uxFrdzx` and `cisco-sa-sdwan-arbfw-c2rZvQ` 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 released software fixes for these vulnerabilities on all release trains at this time,

---

but 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. Upgrade to a fixed software version and adhere to TAC guidance regarding any other necessary next steps.

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 both advisories (CVE-2026-20245 and CVE-2026-20262).

For advisory CVE-2026-20245, the analysis is focused on a specific log entry in **/var/log/scripts.log** on each control component (vManage, vSmart, and vBond). 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 your normal operational posture before being treated as a confirmed indicator.

For advisory CVE-2026-20262, the analysis is focused on several files in the **/var/log/nms** directory of each Manager (vManage). In some instances, these indicators of compromise can occur during standard operations.

These logs do not distinguish between legitimate and malicious use; therefore, any matching entries require manual review by TAC against your 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 either advisory were observed. No further action specific to these advisories is required at this time. The result is limited to the admin-tech files received and is subject to the log retention period on each device.
- **Matching log entries identified** — TAC engages the user with additional review steps. An upgrade to a fixed release is recommended for both advisories. Due to the nature of the advisories, additional action can also be required. TAC's guidance for confirmed-compromise scenarios is documented in the related TechZone articles referenced in Step 4.



Note: Per the CVE-2026-20245 advisory, exploitation requires *netadmin* privileges, while CVE-2026-20262 requires at least a lower-privileged single-task user account. An unauthenticated attacker can obtain those credentials 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 both CVE-2026-20245 and CVE-2026-20262 are mitigated on those specific devices, based on the files reviewed.

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

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

If no indicators of compromise are identified for either advisory, no further action specific to the

compromise assessment is required at this time, based on the admin-tech files reviewed. Upgrading to a fixed release for both advisories is still strongly recommended.

Fixed Software Versions

These software releases contain fixes for the identified vulnerabilities:

Applies to Current Versions	Fixed Version	Available Software
20.9.9.1 and earlier	**20.9.9.2**	20.9.9.2 upgrade images for vManage, vSmart and vBond
20.12.7.1 and earlier	**20.12.7.2**	20.12.7.2 upgrade images for vManage, vSmart, and vBond
20.15.4.4 and earlier	**20.15.4.5**	20.15.4.5 upgrade images for vManage, vSmart, and vBond
20.15.5.2 and earlier	**20.15.5.3**	20.15.5.3 upgrade images for vManage, vSmart, and vBond
20.16, 20.17, 20.18.x	**20.18.3.1**	20.18.3.1 upgrade images for vManage, vSmart, and vBond
26.1	**26.1.1.2**	26.1.1.2 upgrade images for vManage, vSmart, and vBond

---



Note: For customers on CDCS (Cisco-Hosted Cluster), 20.15.507 is also a fixed release. This applies specifically to the Cisco-hosted cluster deployment and is handled separately from the standard upgrade path.

Important References:

- Upgrade Matrix
- Controller Compatibility Matrix
- Remediate Catalyst SD-WAN Security Advisory — May 2026
- Remediate Catalyst SD-WAN Security Advisory — February 2026
- Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability (May 14, 2026)

Considerations

At the conclusion of a successful remediation, and based on your specific security assurance requirements, Cisco recommends that you evaluate and act on the hygiene activities listed here. These activities apply regardless of which remediation option is selected. They are user-managed; Cisco does not direct or perform them on your 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 each customer.



Note: Where compromise of an edge device is suspected, a factory reset and re-onboarding of the affected edge device(s) is a customer-managed action to take into account when making your selection. The decision whether to pursue this approach, and which option to select, rests with each customer.

The proper command to perform a secure factory reset is:

```
factory-reset all secure
```

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 shown here 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 both advisories, the manual verification consists of targeted log checks. The log entries targeted by these checks are generated by **legitimate** commands and activity, and the logs alone do not distinguish between legitimate and malicious use. Any matching entry must be reviewed against your 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 for CVE-2026-20245: Check `scripts.log` on each control component for File

Upload Entries

Per the PSIRT advisory, users are encouraged to audit log files for entries similar to these examples. On release 20.9 and later, these entries are found in `scripts.log` at `/var/log/`. On releases prior to 20.9, the equivalent data is found in `vdebug` logs at `/var/log/tmplog/`.

Three distinct legitimate upload commands produce entries in this same log with the same format. Each must be audited:

Example entry for a tenant list upload — `vconfd_script_upload_tenant_list.sh`:

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

Example entry for a vSmart serial numbers upload — `vconfd_script_upload_vsmart_serial_numbers.sh`:

```
Jun  5 13:06:39 Manager vScript: vSmart upload serial numbers: /usr/bin/vconfd_script_upload_vsmart_ser
```

Example entry for a ZTP chassis numbers upload — `vconfd_script_upload_chassis_number_file.sh`:

```
Jun  5 13:08:47 Validator vScript: ZTP upload chassis numbers: /usr/bin/vconfd_script_upload_chassis_nu
```

Step 1: Access vshell on each control component and search the appropriate log files for CVE-2026-20245 indicators

The log file location depends on the software release running on the control component. Determine which applies to your environment before running the search.

The search commands below use the broadened pattern `vconfd_script_upload_.*\.sh` so a single invocation per log location catches all three upload scripts named above (`vconfd_script_upload_tenant_list.sh`, `vconfd_script_upload_vsmart_serial_numbers.sh`, and `vconfd_script_upload_chassis_number_file.sh`).

Release 20.9 and later — Search `scripts.log` in the `/var/log/tmplog/`:

From the vManage CLI, drop into vshell and run:

```
vs
zgrep -E "vconfd_script_upload_.*\.sh" /var/log/scripts.log*
```

Releases prior to 20.9 — Search `vdebug` logs in `/var/log/tmplog/`:

On releases prior to 20.9, `scripts.log` is not present. The equivalent log data is written to `/var/log/tmplog/vdebug`. Up to five rolling numbered files are retained (`vdebug`, `vdebug.1` through `vdebug.5`). Search all active files with:

```
vs
zgrep -E "vconfd_script_upload_.*\.sh" /var/log/tmplog/vdebug*
```

In addition to the active files, older logs are archived as compressed tar files in `/var/log/` using the naming pattern `vdebug_<timestamp>.tar.gz`, with the log data stored inside the archive at `var/log/tmplog`. Search all archives with:

```
for f in /var/log/vdebug_*.tar.gz; do echo "=== $f ==="; tar -xOf "$f" var/log/tmplog 2>/dev/null | gre
```

Repeat all applicable checks on each control component 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 your normal operational posture. The underlying commands (tenant list upload, vSmart serial numbers upload, and ZTP chassis numbers upload) are legitimate and 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 is a potential 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, refer to the flow described in the related TechZone documents: and remediation guides.

Verification for CVE-2026-20262: Check Log Files on each Manager (vManage) for Arbitrary File Write Entries

Per the PSIRT advisory, users are encouraged to audit these log files on each Manager (vManage) for entries similar to these examples:

Example suspicious entry in `vmanage-server.log` (located at `/var/log/nms/`)

```
11-June-2026 03:53:37,310 EDT INFO  [a66cdc5f-807d-4c23-944e-5c809a2ece6b] [server] [SdraAnyConnectFile
```

Example suspicious entry in `vmanage-appserver.log` (located at `/var/log/nms/`)

```
11-June-2026 07:52:55,275 UTC INFO  [server] (DeploymentScanner-threads - 2) WFLYSRV0010: Deployed "sus
```

Example suspicious entry in `serviceproxy-access.log` (located at `/var/log/nms/containers/service-proxy/`)

```
POST /suspicious/index.jsp HTTP/1.1
```



Note: On releases prior to 20.9, `serviceproxy-access.log` is located at `/var/log/nms/` rather than `/var/log/nms/containers/service-proxy/`.

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

From the vManage CLI, drop into vshell and run :

```
vs
zgrep "SdraAnyConnectFileUploadHandler" /var/log/nms/vmanage-server.log*
zgrep "WFLYSRV0010" /var/log/nms/vmanage-appserver.log*
```

On some releases, the service-proxy log is accessible directly from vshell. On releases where root shell access is required, download the admin-tech and search the `serviceproxy-access.log` files within it in the same way using a command similar to:

Release 20.9 and later:

```
tar -xOf <admin-tech-filename>.tar.gz var/log/nms/containers/service-proxy/serviceproxy-access.log 2>/d
```

Releases prior to 20.9:

```
tar -xOf <admin-tech-filename>.tar.gz var/log/nms/serverproxy-access.log 2>/dev/null | grep "suspicious
```

If accessing directly from vshell, use the .war filename identified from the results of the previous two commands (without the extension) in place of `suspicious`:

Release 20.9 and later:

```
zgrep "POST" /var/log/nms/containers/service-proxy/serviceproxy-access.log* | grep "suspicious"
```

Releases prior to 20.9:

```
zgrep "POST" /var/log/nms/serverproxy-access.log* | grep "suspicious"
```

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 files 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 your normal operational posture. These entries can occur during standard operations and do not on their own confirm compromise.
- For each matching entry in `vmanage-server.log`, capture the timestamp, the full log line, and the file path referenced in the upload handler.
- If a matching entry cannot be reconciled with a known, legitimate operation, this is a potential 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, refer to the flow described in the related TechZone documents: and remediation guides.

Frequently Asked Questions

Q: What is the first step to address these security advisories?

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 these vulnerabilities?

A: Yes, fixed releases are available for both advisories, as listed in the Fixed Software Versions section. There are no workarounds.

Q: Why does Cisco recommend taking action beyond upgrading?

A: Exploitation of these vulnerabilities requires an authenticated user. An unauthenticated attacker can obtain those credentials 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 these vulnerabilities. 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 these advisories?

A: TAC reviews the admin-tech files for indicators of compromise specific to each advisory. For the privilege escalation advisory (CVE-2026-20245), TAC looks for specific log entries in `/var/log/scripts.log` on each control component. For the arbitrary file write advisory (CVE-2026-20262), TAC looks for specific log entries across three log files on each Manager: `/var/log/nms/vmanage-server.log`, `/var/log/nms/vmanage-appserver.log`, and `/var/log/nms/containers/service-proxy/serviceproxy-access.log`. In both cases, the underlying activity can occur during standard operations; any matching entries are reviewed by TAC against your normal operational posture before being treated as a confirmed indicator.

Q: What happens if indicators of compromise are identified?

A: TAC contacts you with specific guidance. The upgrade alone does not resolve a confirmed compromise. TAC's guidance is based on 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 these advisories?

A: These advisories primarily affect Cisco Catalyst SD-WAN control components. For the privilege escalation advisory (CVE-2026-20245), all control components (vManage, vSmart, vBond) are affected, and Cisco has observed limited cases where exploitation resulted in a configuration change being pushed to edge devices; users are encouraged to verify the configuration of their edge devices. For the arbitrary file write advisory (CVE-2026-20262), the vulnerability is confined to the SD-WAN Manager filesystem and does not directly affect edge devices.

Q: Which deployment types are affected?

A: Per these advisories, these vulnerabilities affect all Cisco Catalyst SD-WAN 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 these new vulnerabilities?

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 both CVE-2026-20245 and CVE-2026-20262 are mitigated on those specific devices, based on the files reviewed. This does not eliminate exposure where an attacker holds valid credentials. Cisco recommends you upgrade to a fixed release for these advisories.

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

A: Users who cannot share admin-techs can 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 these vulnerabilities?

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