Remediate Catalyst SD-WAN Security Advisory - February 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: Execute Remediation (TAC-Guided)

- Path A: No Indicators of Compromise Found — Upgrade
- Path B: Indicators of Compromise Identified — PSIRT-Guided

Fixed Software Versions

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

- Verification 1: Check for Unauthorized SSH Logins in Auth Logs
- Verification 2: Check for Unauthorized Peer Connections in Controller Syslogs
- Verification 3: DCA File Read
- Verification 4: Path Traversal / Arbitrary File Overwrite
- Verification 5: File Deployment

Frequently Asked Questions

Introduction

This document describes steps to identify and fix critical security vulnerabilities in SD-WAN based on PSIRT advisories dated Feb 25, 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 Vulnerabilities
- Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability

These defects are addressed by these PSIRT advisories:

- Cisco bug ID CSCws52722
- Cisco bug ID CSCws33583
- Cisco bug ID CSCws33584
- Cisco bug ID CSCws33585
- Cisco bug ID CSCws33586
- Cisco bug ID CSCws33587
- Cisco bug ID CSCws93470

Remediation Workflow Overview



Note: All SD-WAN deployments are vulnerable and require immediate action. However, not all systems show evidence of compromise.

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
- Work with the PSIRT team if indicators of compromise are identified
- Provide upgrade guidance and support if no indicators of compromise are detected

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 assesses your environment for indicators of compromise
4. **Execute Remediation** - Complete the specific process provided by TAC

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

Required: Collect admin-tech files from all control components before opening your TAC case. This is essential for TAC to assess your environment.

Collection:



Note: 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)



Note: vSmart admin-techs must not be run simultaneously — collect them one at a time. Admin-techs for Managers and Validators can be collected in any order.

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 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: Open a TAC Case and Upload Admin-Tech Files

After collecting all admin-tech files from Step 1, **open a Cisco TAC support case**.

Required Actions:

1. Open a TAC case with severity level appropriate to your business impact
2. Upload ALL admin-tech log bundles collected in Step 1 (Controllers, Managers, and Validators)
3. Reference the PSIRT advisories
4. Wait for TAC assessment and guidance



Caution: TAC determines the status of your system and recommends appropriate next steps.

Do not attempt further steps without TAC guidance

Step 3: TAC Assessment

TAC analyzes the uploaded admin-tech files and determines the status of your system.

During this time:

- Wait for an official assessment from TAC before taking any action
- TAC contacts you with their findings and next steps

Step 4: Execute Remediation (TAC-Guided)

TAC guides you through the appropriate remediation process based on their assessment. Complete all instructions provided by TAC.

Path A: No Indicators of Compromise Found — Upgrade

If TAC confirms there is no evidence of compromise, upgrade to the fixed software version. Select the appropriate version from the Fixed Software Versions table in this document and reference the upgrade guide linked in this section.

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

Path B: Indicators of Compromise Identified — PSIRT-Guided

If TAC confirms indicators of compromise are present, complete all guidance provided by TAC.

Fixed Software Versions

These software releases contain fixes for the identified vulnerabilities:

Applies to Current Versions	Fixed Version	Available Software
20.3, 20.6, 20.9	**20.9.8.2** *	20.9.8.2 upgrade images for vManage, vSmart, and vBond
20.10, 20.11, 20.12.5 and earlier in 20.12	**20.12.5.3**	20.12.5.3 upgrade images for vManage, vSmart, and vBond

Applies to Current Versions	Fixed Version	Available Software
20.12.6	**20.12.6.1**	20.12.6.1 upgrade images for vManage, vSmart, and vBond
20.13, 20.14, 20.15.x	**20.15.4.2**	20.15.4.2 upgrade images for vManage, vSmart, and vBond
20.16, 20.17, 20.18.x	**20.18.2.1**	20.18.2.1 upgrade images for vManage, vSmart, and vBond

Note: For customers on **CDCS (Cisco-Hosted Cluster)**, **20.15.405** is also a fixed release. This applies specifically to the Cisco-hosted cluster deployment and is handled separately from the standard upgrade path.

*** If you are on release 20.9 or earlier:** The fixed software for your release (20.9.8.2) is available on 2/27. Cisco recommends remaining within your current major release and waiting for the 20.9.8.2 release rather than upgrading to a higher major release (20.12, 20.15, 20.18). If you are currently in a version lower than 20.9, wait for 20.9.8.2 to upgrade there. Continue to work with TAC and check back on 2/27 for the available software link.

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 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.

Note:

- 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 control components.

Verification 1: Check for Unauthorized SSH Logins in Auth Logs

Step 1: Identify Valid vManage System IPs

Access each vSmart controller and execute:

```
west-vsmart# show control connections | inc "vmanage|PEER|IP"
```

Example output:

```
                                                  PEER
      PEER  PEER  PEER            SITE       DOMAIN  PRIV    PEER                          PUB
INDEX TYPE  PROT  SYSTEM IP       ID         ID      PRIVATE IP                    PORT    PUBLIC I
-----------------------------------------------------------------------------------------------
0     vmanage dtls 10.1.0.18     101018     0       10.1.10.18                    12346   10.1.10.1
```

Step 2: Build Regular Expression String (vBond and vSmart only)

Combine all system IPs from Step 1 into an OR regex pattern:

```
system-ip1|system-ip2|...|system-ipn
```

Step 2b: Additional Step for vManage Systems

If running these commands on vManage itself, append the localhost IP (127.0.0.1), local system IP, all cluster IPs, and the VPN 0 transport interface IP to the regex:

```
system-ip1|system-ip2|...|system-ipn|127.0.0.1|<local-system-ip>
```

To find the local vManage system IP, use:

```
show control local-properties
```

To find the VPN 0 transport interface IP and cluster IP, use:

```
show interface | tab
```

Step 3: Execute Verification Command

Run this command, replacing `REGEX` with your regex string from Step 2:

```
west-vsmart# vs
west-vsmart:~$ zgrep "Accepted publickey for vmanage-admin from " /var/log/auth.log* | grep -vE "\s(REG
```



Note: This command filters authentication logs to show only vmanage-admin logins from unexpected sources. Legitimate logins must only originate from vManage related IPs.

Step 4: Interpret Results and Document for TAC

If NO output is displayed:

- No indicators of compromise detected on this device
- Document this result for your TAC case
- Continue assessment on remaining controllers

If log lines are printed:

- Carefully examine each IP address shown
- Verify the IP is not related to vManage infrastructure (cluster IP, old system IP, or similar)
- If you cannot identify the source IP as legitimate, this can indicate potential indicators of compromise
- The log entry shows a timestamp and source IP address
- **Document all findings and open a TAC case immediately**
- Include the log entries, timestamps, and source IPs in your case
- TAC performs the official assessment determination

Verification 2: Check for Unauthorized Peer Connections in Controller Syslogs

This command extracts all peer-type and peer-system-ip pairs from controller syslog files and outputs them as a list for you to review. It does not automatically flag suspicious entries — you must inspect the output and determine whether each peer system IP is a known, legitimate part of your SD-WAN infrastructure. Run this on all control components (Controllers, Managers, and Validators).

Step 1: Run the command on each control component:

First, access vshell and navigate to the log directory:

```
vs
cd /var/log
```

Then run the this command:

```
awk '{
```

```
  match($0, /peer-type:([a-zA-Z0-9]+)[^ ]* peer-system-ip:([0-9.:]+)/, arr);
  if(arr[1] && arr[2]) print "(" arr[1] ", " arr[2] ")";
}' vsyslog* | sort | uniq
```

Step 2: Interpret Results and Document for TAC

If output only shows known vManage/vSmart/vBond system IPs:

- No indicators of compromise detected from this check
- Document this result for your TAC case
- Continue assessment on remaining control components

If output contains unrecognized peer system IPs:

- Carefully examine each IP address and peer-type shown
- Verify the IP is not related to your known SD-WAN control plane infrastructure
- 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 full command output with peer-type and peer-system-ip pairs in your case
- TAC performs the official assessment determination

Verification 3: DCA File Read

Step 1: What to Look For

Log file: `/var/log/nms/containers/service-proxy/serviceproxy-access.log`

Example log line:

```
[2026-03-04T01:45:06.239Z] "GET /reports/data/opt/data/containers/config/data-collection-agent/.dca HTT
```

Note: IOC3 does not use HTTP status code as a gating condition. Any traversal attempt is recorded. The status code is still relevant for analyst interpretation (for example, HTTP 200 indicates successful file read), but non-200 responses remain exploitive attempts and must be assessed.

Step 2: Manual Search Command

From Terminal — search within extracted admin-tech bundle:

```
zgrep -r "data-collection-agent/.dca" var/log/nms/containers/service-proxy/serviceproxy-access.log*
```

Note: Legitimate DCA administration can include the `.dca` URI from known administrator IP

---

addresses. Always validate source IP addresses against known administrator sources before escalation. Treat any unrecognized source IP for either sub-type as suspicious.

Verification 4: Path Traversal / Arbitrary File Overwrite



Note: IOC4 applies only to vManage devices. Any `SmartLicensingManager` log entry writing a file via `../` traversal is flagged regardless of outcome. If the write entry exists in the log, the write occurred.

Step 1: What to Look For

Log file: `/var/log/nms/vmanage-server.log`

Example log lines:

```
06-Mar-2026 02:16:34,029 UTC INFO  [285fcdc0-30fa-4ca0-8e06-6953a095a59a] [LAB-TEST-1] [SmartLicensingM
04-Mar-2026 15:40:02,683 IST INFO  [ca0e641b-acc7-42a6-b39b-bf3d28be0bcb] [LAB-TEST-1] [SmartLicensingM
27-Feb-2026 08:49:27,169 IST INFO  [d9976a9d-071e-4e07-a3ef-4e90019cae12] [LAB-TEST-1] [SmartLicensingM
```

Caution: The filename shown in examples (for example, `cmd.gz.war`) is illustrative only. Actual cases can use different filenames. Record all unique traversal filenames identified, as each represents a separate dropped payload.

Step 2: Manual Search Command

From Terminal — search within extracted admin-tech bundle:

```
grep -rE "SmartLicensingManager.*Time taken to write file \.\.\/" var/log/nms/vmanage-server.log*
```

Including rotated/compressed logs:

```
zgrep -E "SmartLicensingManager.*Time taken to write file \.\.\/" var/log/nms/vmanage-server.log*
```

To capture related context lines (upload API processing and write events):

```
grep -rE "SmartLicensingManager.*(write file|is processing|stringUrl|Failed to download).*/wildfly" var
```

Verification 5: File Deployment

Caution: File extensions seen in a compromised environment can vary. The examples and search patterns covered common scenarios but are not exhaustive.

Step 1: What to Look For

Log file: `/var/log/nms/containers/service-proxy/serviceproxy-access.log`

Any POST request to a `*.gz/*.jsp` URI pattern is flagged. HTTP status determines severity:

HTTP Status	Meaning	Confirmed Compromise?
200	Server executed the webshell; payload is active	Yes - confirmed compromise

Example log lines:

```
[2026-03-04T08:03:33.295Z] "POST /cmd.gz/cmd.jsp HTTP/1.1" 200 - 6 63 78 - "<source_IP_address>" "pytho
```

Step 2: Manual Search Command

From Terminal — search within extracted admin-tech bundle:

```
grep -rE '"POST /[^"]+\.gz/[^"]+\.jsp HTTP' var/log/nms/containers/service-proxy/serviceproxy-access.lo
```

Including rotated/compressed logs:

```
zgrep -E '"POST /[^"]+\.gz/[^"]+\.jsp HTTP' var/log/nms/containers/service-proxy/serviceproxy-access.lo
```

To separate confirmed execution (HTTP 200) from non-200 attempts:

```
# HTTP 200 only - confirmed webshell execution:
grep -rE '"POST /[^"]+\.gz/[^"]+\.jsp HTTP[^"]*" 200' var/log/nms/containers/service-proxy/serviceproxy
```

Note: Document all unique source IPs, total request count, and count of HTTP 200 responses. Report to Cisco TAC.

Frequently Asked Questions

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

A: Collect admin-tech files from all control components and open a TAC case to upload the files. TAC assesses your environment and provides guidance on next steps.

Q. What version do I need to I upgrade to?

A. Please upgrade to the nearest fixed version at the earliest.

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 properly assess your environment.

Q: How does TAC determine if my system has been compromised?

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

Q: What happens if indicators of compromise are identified?

A: 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.

Q: How do I know which fixed software version to use?

A: Refer to the Fixed Software Versions table in this document. TAC confirms the appropriate version for your specific environment.

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

A: No, wait for TAC to complete their assessment and provide guidance before attempting any remediation actions.

Q: Is downtime expected during remediation?

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

Q: Are the PSIRT fixes included in the upcoming 20.15.5 release and other upcoming releases?

A: Yes, fixes are included in 20.15.5 and other upcoming releases. However, the upgrade to mitigate the vulnerabilities outlined in this document must be prioritized IMMEDIATELY. (Do not wait!)

Q: Do all controllers need to be upgraded in case no indicators of compromise are found?

A: Yes, all SD-WAN control components (vManage, vSmart, and vBond) must be upgraded to a fixed software version. Upgrading only a subset of controllers is not sufficient.

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

A: 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.

Q: Do we need to upgrade the edge routers as well?

A: Cisco IOS XE devices are not affected by this advisory.

Q: We are a Cisco hosted overlay. Do we need to fix any ACLs or take action on SSP?

A: All Cisco-hosted customers are advised to review their own Allowed Inbound Rules seen on SSP and ensure only the necessary prefixes from your side are allowed. These rules are for management access only and that these rules do not apply for edge routers. Please review them in SSP > Overlay Details > Allow Inbound rules. Please note that port 22, 830 were always blocked by default on Day 0 provisioning by Cisco from outside to the cloud hosted controllers.

Q: We are on CDCS / Shared tenant. What version are we going to be upgraded to?

A: Based on the current version, the Shared Tenant or CDCS clusters are currently on schedule to be upgraded OR already upgraded to the fixed versions. Here are the shared tenant and CDCS fixed releases:

1. Early Adopter clusters => 20.18.2.1 (this is actually same as the standard release)

2. Recommend release clusters => 20.15.405 (CDCS specific version with PSIRT fixes)

CDCS customers dont need to take any action effectively to address this PSIRT.

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

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

Q: We see logs from a "root" user on our system. Is this concerning?

A: Check what else is going on in the system at the time. These logs can be completely expected. For example, system-login-change logs from a "root" user are seen when admin-techs are generated. Logs can also be seen from a "root" user during a reboot.

```
Feb 28 23:03:44 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-
Feb 28 23:03:47 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-
```

Q: We have already upgraded with no indicators of compromise. After the new IOCs were released on March 17, what do I need to do?

A: The software listed as fixed contains protection against further attempts to exploit the CVEs listed in the two advisories covered in this article. While upgrade protects against future exploits, there could be existing exploits which are still in place that occurred prior to the upgrade. It is recommended that customers use the self-service "Check Bug Applicability" which is built-in on the Bug Search Tool Page for Cisco bug ID CSCws52722 to rescan admin-techs from the Control Components. If needed, customers can open a TAC case and repeat the process described in this article to rescan admin-techs based on the new IOCs. b