Remediate Catalyst SD-WAN Security Advisory - May 2026

Contents

Introduction

This document describes steps to identify and fix critical security vulnerabilities in SD-WAN based on PSIRT advisories dated May 14, 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 Authentication Bypass Vulnerability
- Cisco Catalyst SD-WAN Vulnerabilities

These defects are addressed by these PSIRT advisories:

- Cisco bug ID CSCwt50498
- Cisco bug ID CSCwt38739
- Cisco bug ID CSCwt38767
- Cisco bug ID CSCwt55544

Remediation Workflow Overview

Note: All SD-WAN Controllers and Managers are vulnerable and require an immediate upgrade for all Control Components. However, not all controllers show evidence of compromise.

Required Action: Collect admin-techs, upgrade to a fixed release, and then 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 control components (vSmart, vManage, vBond) **prior to the upgrade to ensure no diagnostic data is lost.** Select Log and Tech options. Core is not required.

   Caution: vSmart admin-techs must not be run simultaneously — run them one at a time. All others can be collected in any order

   ---

2. **Upgrade to a Fixed Release** - Upgrade all SD-WAN control components (vManage, vSmart, vBond) to a fixed software version listed in the Fixed Software Versions table.

   Note: 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, Follow 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 Control Components

Required: Collect admin-tech files from all control components 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:

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: Upgrade to a Fixed Software Version

After collecting admin-techs in Step 1, upgrade all SD-WAN control components (vManage, vSmart, and vBond) 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

Note: 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 "CVE-2026-20182" and the relevant PSIRT ID in the title to initiate the scanning process.
2. Upload ALL admin-tech log bundles collected in Step 1 (Controllers, Managers, and Validators)
3. Wait for TAC to complete the scan and communicate the results

Note: 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 — Follow 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 fixes for the identified vulnerabilities:

Applies to Current Versions	Fixed Version	Available Software
20.3, 20.6, 20.9	**20.9.9.1**	20.9.9.1 upgrade images for vManage, vSmart, and vBond
20.10, 20.11, 20.12.5 and earlier in 20.12	**20.12.5.4**	20.12.5.4 upgrade images for vManage, vSmart, and vBond
20.12.6.x	**20.12.6.2**	20.12.6.2 upgrade images for vManage, vSmart, and vBond
20.12.7	**20.12.7.1**	20.12.7.1 upgrade images for vManage, vSmart, and vBond
20.13, 20.14, 20.15.4.3 and earlier in 20.15	**20.15.4.4**	20.15.4.4 upgrade images for vManage, vSmart, and vBond
20.15.5.x	**20.15.5.2**	20.15.5.2 upgrade images for vManage, vSmart, and vBond
20.16, 20.17, 20.18.x	**20.18.2.2**	20.18.2.2 upgrade images for vManage, vSmart, and vBond

Note: For customers on **SD-WAN Cloud (formerly known as Cloud Delivered Cisco Catalyst SD-WAN [CDCS])**, the 20.15.506 is also a fixed release. This applies specifically to the Cisco-hosted cluster deployment and is handled separately from the standard upgrade path. All such customers are already upraded to the fixed release 20.15.506.

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 to search the vsyslog* file glob:

```
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
```

Repeat this for **messages*** file glob as well as **vdebug*** file glob.

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: Check for Missing challenge-ack on Active Control Connections

This check inspects the **control connections detail** output for peer sessions that are reported as active (or recently torn down) but are missing the expected `challenge-ack` exchange. A session that exchanges `hello` packets in both directions while showing `challenge-ack 0` in either the Tx or Rx statistics indicates the peer never completed the expected challenge handshake — an anomaly that warrants investigation. Run this on all control components (Controllers, Managers, and Validators).

Step 1: Collect the control connections detail output

From the device CLI, run:

```
show control connections detail
show control connections-history detail
```

Save the output to a file (for example, `vdaemon.txt`) for inspection.

Step 2: What to look for

For each peer record (delimited by `REMOTE-COLOR-` / `SYSTEM-IP-` headers), flag the record if **all** of these conditions are true:

- Session **state** is **UP** or **TEAR_DOWN**
- Both the **Tx Statistics hello** counter and the **Rx Statistics hello** counter are non-zero (hellos are flowing in both directions)
- **challenge-ack** is **0** in either the **Tx Statistics** or **Rx Statistics** block (or both)

Example matching record (note the `<<<<` arrows highlighting the missing `challenge-ack`)

```
-----------------------------------------------------------------------------------------------
 REMOTE-COLOR- default SYSTEM-IP- 10.2.2.2   PEER-PERSONALITY- vmanage
-----------------------------------------------------------------------------------------------
site-id             432567
domain-id           0
protocol            dtls
private-ip          10.0.0.1
private-port        12346
public-ip           192.168.1.1
public-port         50825
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:16:58
hello interval      1000
hello tolerance     12000

  Tx Statistics-
  --------------
    hello                   3423293
    challenge               1
    challenge-response      0
    challenge-ack           0           <<<< MISSING challenge-ack (Tx)
    ...

  Rx Statistics-
  --------------
    hello                   3423291
    challenge               0
    challenge-response      1
    challenge-ack           0           <<<< MISSING challenge-ack (Rx)
    ...
```

In the example above, both Tx and Rx `hello` counters are non-zero (active connection), but `challenge-ack` is `0` in both directions.

Step 3: Manual Search Command

To quickly surface candidate records from a saved `vdaemon.txt` (or any file containing the `show control connections detail` output), run:

```
grep -A20 'SYSTEM-IP' vdaemon.txt | grep -B5 'challenge-ack  0'
```

Each block returned represents a peer session where `challenge-ack` is reported as `0`. Review each block in full to confirm `state` is `up` or `tear_down` and that the `hello` counters in both Tx and Rx are non-zero before treating it as a hit.

Step 4: Interpret Results and Document for TAC

If no records meet all three conditions:

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

If one or more records meet all three conditions:

- Carefully examine the `SYSTEM-IP-`, `private-ip`, and `public-ip` values for each flagged record
- Verify the peer is not a known, legitimate part of your SD-WAN control plane (cluster member, DR site, IP address previously assigned to a component)
- If you cannot identify the peer as legitimate, this can indicate potential indicators of compromise
- **Document all findings and open a TAC case immediately**
- Include the full matching peer record(s) and the source command output in your case
- TAC performs the official assessment determination

Frequently Asked Questions

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

A: Collect admin-tech files from all control components, then upgrade all control components 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.

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: 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.

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: 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: No, 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 SD-WAN Cloud (formerly known as Cloud Delivered Cisco Catalyst SD-WAN [CDCS]). What version are we going to be upgraded to?

A: Based on the current version, SD-WAN Cloud clusters are currently on schedule to be upgraded OR already upgraded to the fixed versions. Here are the SD-WAN Cloud (formerly CDCS) fixed releases:

1. Early Adopter clusters = 20.18.2.2 (this is actually same as the standard release)

2. Recommend release clusters = 20.15.506 (CDCS specific version with PSIRT fixes)

SD-WAN Cloud customers do not need to take any action effectively to address this PSIRT.

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

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

1. Recommend release clusters = 20.15.5.2

Q: Does Cisco TAC provide forensic analysis or investigation services for these vulnerabilities?

A: Cisco TAC can assist customers by scanning for Indicators of Compromise (IoCs) related to these

vulnerabilities. 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.

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-
```