Cisco Security Advisory

Cisco Catalyst SD-WAN Vulnerabilities

Critical

Advisory ID:
cisco-sa-sdwan-authbp-qwCX8D4v

First Published:
2026 February 25 16:00 GMT

Last Updated:
2026 March 18 01:06 GMT

Version 1.2: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCws33583 , CSCws33584 , CSCws33585 , More...

CVE-2026-20122

CVE-2026-20126

CVE-2026-20128

More...

CWE-200

CWE-257

CWE-287

More...

CVSS Score:
Base 9.8

Download CSAF

Email

Summary

Multiple vulnerabilities in Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an attacker to access an affected system, elevate privileges to *root,* gain access to sensitive information, and overwrite arbitrary files.

For more information about these vulnerabilities, see the Details section of this advisory.

Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.

Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v

Affected Products

Vulnerable Products

These vulnerabilities affect Cisco Catalyst SD-WAN Manager, regardless of device configuration.

For information about which Cisco software releases are vulnerable, see the Fixed Software section of this advisory.

Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by these vulnerabilities.

Cisco has confirmed that Cisco Catalyst SD-WAN Manager releases 20.18 and later are not affected by the vulnerabilities that are described in CVE-2026-20128 and CVE-2026-20129.

Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

Details

These vulnerabilities are not dependent on one another. Exploitation of one of th
vulnerability.

Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

Details about the vulnerabilities are as follows:

CVE-2026-20129: Cisco Catalyst SD-WAN Manager Authentication Bypass Vulnerability

A vulnerability in the API user authentication of Cisco Catalyst SD-WAN Manager could allow an unauthenticated, remote attacker to gain access to an affected system as a user who has the *netadmin* role.

The vulnerability is due to improper authentication for requests that are sent to the API. An attacker could exploit this vulnerability by sending a crafted request to the API of an affected system. A successful exploit could allow the attacker to execute commands with the privileges of the *netadmin* role.

Note: Cisco Catalyst SD-WAN Manager releases 20.18 and later are not affected by this vulnerability.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Bug ID(s): CSCws33587
CVE ID: CVE-2026-20129
Security Impact Rating (SIR): Critical
CVSS Base Score: 9.8
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2026-20126: Cisco Catalyst SD-WAN Manager Privilege Escalation Vulnerability

A vulnerability in Cisco Catalyst SD-WAN Manager could allow an authenticated, local attacker with low privileges to gain *root* privileges on the underlying operating system.

This vulnerability is due to an insufficient user authentication mechanism in the REST API. An attacker could exploit this vulnerability by sending a request to the REST API of the affected system. A successful exploit could allow the attacker to gain *root* privileges on the underlying operating system.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Bug ID(s): CSCws93470
CVE ID: CVE-2026-20126
Security Impact Rating (SIR): High
CVSS Base Score: 7.8
CVSS Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2026-20133: Cisco Catalyst SD-WAN Manager Information Disclosure Vulnerability

A vulnerability in Cisco Catalyst SD-WAN Manager could allow an unauthenticated, remote attacker to view sensitive information on an affected system.

This vulnerability is due to insufficient file system access restrictions. An attacker could exploit this vulnerability by accessing the API of an affected system. A successful exploit could allow the attacker to read sensitive information on the underlying operating system.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Bug ID(s): CSCws33583
CVE ID: CVE-2026-20133
Security Impact Rating (SIR): High
CVSS Base Score: 7.5
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVE-2026-20122: Cisco Catalyst SD-WAN Manager Arbitrary File Overwrite Vulnerability

A vulnerability in the API of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to overwrite arbitrary files on the local file system. To exploit this vulnerability, the attacker must have valid *read-only* credentials with API access on the affected system.

This vulnerability is due to improper file handling on the API interface of an affected system. An attacker could exploit this vulnerability by uploading a malicious file on the local file system. A successful exploit could allow the attacker to overwrite arbitrary files on the affected system and gain *vmanage* user privileges.

Cisco has released software updates that address this vulnerability. There are no

Bug ID(s): CSCws33584, CSCws33586
CVE ID: CVE-2026-20122
Security Impact Rating (SIR): High
CVSS Base Score: 7.1
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L

CVE-2026-20128: Cisco Catalyst SD-WAN Manager Information Disclosure Vulnerability

A vulnerability in the Data Collection Agent (DCA) feature of Cisco Catalyst SD-WAN Manager could allow an unauthenticated, remote attacker to gain DCA user privileges on an affected system.

This vulnerability is due to the presence of a credential file for the DCA user on an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request and reading the file that contains the DCA password from that affected system. A successful exploit could allow the attacker to access another affected system and gain DCA user privileges.

Note: Cisco Catalyst SD-WAN Manager releases 20.18 and later are not affected by this vulnerability.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Bug ID(s): CSCws33585
CVE ID: CVE-2026-20128
Security Impact Rating (SIR): High
CVSS Base Score: 7.5
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Indicators of Compromise

Indicators of compromise for the exploitation of CVE-2026-20128 and CVE-2026-20122 are as follows.

CVE-2026-20128: Cisco Catalyst SD-WAN Manager Information Disclosure Vulnerability

Customers are encouraged to examine log entries in the file */var/log/nms/containers/service-proxy/serviceproxy-access.log* on a Cisco Catalyst SD-WAN Manager for references to */reports/data/opt/data/containers/config/data-collection-agent/.dca*. Legitimate use of this API occurs when administering the DCA and would coincide with this activity. In such a case, the corresponding IP address would be that of the laptop of the administrator.

To identify indicators of compromise and remove false positives, search the file */var/log/nms/containers/service-proxy/serviceproxy-access.log* for log entries such as the following:

```
[2026-03-04T18:14:16.057Z] "GET /reports/data/opt/data/containers/config/data-collection-agent/.dca HTTP/1.1"
200 - 0 32 4 - "172.16.1.1" "python-requests/2.31.0" "7e77bfbc-7224-43e0-9115-cadf13d2fefa" "172.16.0.1"
"127.0.0.1:8080"
```

Compare the log time and source IP (in this example, 172.16.1.1) against known administrator activity to exclude false positives.

CVE-2026-20122: Cisco Catalyst SD-WAN Manager Arbitrary File Overwrite Vulnerability

Examine log entries in the file */var/log/nms/containers/service-proxy/serviceproxy-access.log* on a Cisco Catalyst SD-WAN Manager for references to */dataservice/smartLicensing/uploadAck*. Legitimate use of this API occurs when updating licensing information and would coincide with this activity. In such a case, the corresponding IP address would be that of the laptop of the administrator.

To identify indicators of compromise and remove false positives, search the file */var/log/nms/containers/service-proxy/serviceproxy-access.log* for log entries such as the following:

```
[2026-03-05T14:28:05.106Z] "POST /dataservice/smartLicensing/uploadAck HTTP/1.1" 0 DC 1036 0 10010 -
"10.10.10.23"
```

Compare the log time and source IP (in this example, 10.10.10.23) against known administrator activity to exclude false positives.

If customers see the following POST log example, they should also check the *vmanage-server.log* file for specific filenames being downloaded:

```
[2026-03-05T14:28:05.106Z] "POST /dataservice/smartLicensing/uplo
"10.10.10.23"
```

The following list includes example logs for filenames. Flag them if the file is suspicious.

```
/var/log/nms/vmanage-server.log-03-06-2026-1.gz:06-Mar-2026 02:16:34,029 UTC INFO  [285fcdc0-30fa-4ca0-8e06-
6953a095a59a] [LAB-TEST-1] [SmartLicensingManager] (default task-11229) |57501bad-32a7-4f52-8f54-8547dcd7403e|
Time taken to write file ../../../../../../../../../../../var/lib/wildfly/standalone/deployments/cmd.gz.war = 2
ms to directory /opt/data/app-server/software/package/license/ack
/var/log/nms/vmanage-server.log-03-06-2026-1.gz:06-Mar-2026 02:16:34,029 UTC INFO  [285fcdc0-30fa-4ca0-8e06-
6953a095a59a] [LAB-TEST-1] [SmartLicensingManager] (default task-11229) |57501bad-32a7-4f52-8f54-8547dcd7403e|
../../../../../../../../../../../var/lib/wildfly/standalone/deployments/cmd.gz.war is processing in rpc call
/var/log/nms/vmanage-server.log-03-06-2026-1.gz:06-Mar-2026 02:16:34,094 UTC INFO  [] [sd-wan-manager-0]
[SmartLicensingManager] (pool-187-thread-1) || stringUrl
https://10.0.6.144:8443/software/package/license/ack/../../../../../../../../../../../var/lib/wildfly/standalon
e/deployments/cmd.gz.war filePath
../../../../../../../../../../../var/lib/wildfly/standalone/deployments/cmd.gz.war
/var/log/nms/vmanage-server.log-03-06-2026-1.gz:06-Mar-2026 02:16:34,106 UTC ERROR [] [sd-wan-manager-0]
[SmartLicensingManager] (pool-187-thread-1) || Failed to download the file
../../../../../../../../../../../var/lib/wildfly/standalone/deployments/cmd.gz.war
```

Note: The filename shown here is an example. The actual log entry may contain a different filename.

Customers are also encouraged to check for the presence of file */cmd.gz/cmd.jsp*. Examine log entries in the file */var/log/nms/containers/service-proxy/serviceproxy-access.log* on a Cisco Catalyst SD-WAN Manager for references to */cmd.gz/cmd.jsp*. This is an endpoint that does not exist on a clean Cisco Catalyst SD-WAN Manager but is added by the published proof of concept. Any use of this endpoint is an indicator of compromise, as shown in the following example log:

```
[2026-03-05T14:54:01.541Z] "POST /cmd.gz/cmd.jsp HTTP/1.1" 200 - 6 63 7 - "172.16.1.1" "python-requests/2.31.0"
"7221a300-088a-4a44-84a1-b8388a8ee19e" "172.16.0.1" "127.0.0.1:8080"
```

Note: The filename shown here is an example. The actual log entry may contain a different filename.

Workarounds

There are no workarounds that address these vulnerabilities. Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

Fixed Software

Cisco considers any workarounds and mitigations (if applicable) to be temporary solutions until an upgrade to a fixed software release is available. To fully remediate these vulnerabilities and avoid future exposure as described in this advisory, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

Fixed Releases

In the following tables, the left column lists Cisco software releases. The right column indicates whether a release is affected by the vulnerabilities that are described in this advisory and the first release that includes the fix for these vulnerabilities. Customers are advised to upgrade to an appropriate fixed software release as indicated in this section.

Cisco Catalyst SD-WAN Manager Release	First Fixed Release
Earlier than 20.9[1]	Migrate to a fixed release.
20.9	20.9.8.2
20.10	20.12.6.1
20.11[1]	20.12.6.1
20.12	20.12.5.3 20.12.6.1
20.13[1]	20.15.4.2
20.14[1]	20.15.4.2
20.15	20.15.4.2
20.16[1]	20.18.2.1
20.18	20.18.2.1

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 a ed in this advisory.

Additional Information

- To check component and software release compatibility, see the SD-WAN Controller Component Compatibility Matrix.
- For help planning an upgrade, see the Cisco Catalyst SD-WAN Upgrade Matrix.
- For additional remediation assistance, see Remediate Catalyst SD-WAN Security Advisory - February 2026.
- For additional assistance with requesting the admin-tech bundle for TAC support, see Collect an Admin-Tech in SD-WAN Environment and Upload to TAC Case.
- For additional remediation assistance, see Rebuild Your Catalyst SD-WAN Fabric.

Recommendations

Cisco recommends upgrading the affected systems to a fixed software release.

General Recommendations for Hardening

- Prevent access from unsecured networks, such as the internet, to the system. If internet access to the system is required, restrict system access to only known, trusted hosts on ports/protocols that are included in the user guides.
- Protect Cisco Catalyst SD-WAN Control Components behind a filtering device such as a firewall, and filter traffic to and from the systems while allowing only known, trusted hosts to send traffic to the systems. Using a two-layer firewall can provide flexibility in network planning so that end users do not connect directly to the outer DMZ. See the Deployment sections of the User Guides for Cisco Catalyst SD-WAN software.
- Regularly monitor log traffic for any unexpected traffic to and from systems. Logging should be sent to an external server, if possible, and kept for a long enough duration so that post-event investigations can be performed with sufficient log data.
- Disable HTTP for the Cisco Catalyst SD-WAN Manager web UI administrator portal.
- Disable any network services that are not required, including HTTP and FTP. For more information about specific service functionality, see the Cisco Catalyst SD-WAN user guides.
- Upgrade the system to the latest version of Cisco Catalyst SD-WAN Software.
- Change the default administrator password to a more secure variant. Restrict access to the administrator account by creating user accounts based on necessary access requirements. In addition, create operator accounts for all administrators.
- Use SSL/TLS, obtain an SSL certificate from a certificate authority (CA), or create a self-signed certificate.

For more information, review the Cisco Catalyst SD-WAN Hardening Guide.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities that are described in CVE-2026-20133, CVE-2026-20126, and CVE-2026-20129.

In March 2026, the Cisco PSIRT became aware of active exploitation of the vulnerabilities that are described in CVE-2026-20128 and CVE-2026-20122 only. The vulnerabilities that are described in the other CVEs in this advisory are not known to have been compromised. Cisco strongly recommends that customers upgrade to a fixed software release to remediate these vulnerabilities.

Source

These vulnerabilities were found during internal security testing by Arthur Vidineyev of the Cisco Advanced Security Initiatives Group (ASIG).

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v

Revision History

Version	Description	Section	Status	Date
1.2	Updated the Details section for CVE-2026-20128. Added indicators of compromise for CVE-2026-20128 and CVE-2026-20122. Added Release 20.10 to fixed release table.	Details, Indicators of Compromise, Fixed Releases	Final	2026-MAR-18
1.1	Updated Exploitation and Public Announcements section to include active exploitation of CVE-2026-20128 and CVE-2026-20122. Added links with instructions for uploading admin-tech files into a Cisco TAC case and rebuilding an SD-WAN fabric. Added additional language strongly recommending that customers upgrade to the fixed software indicated in this advisory.	Summary, Vulnerable Products, Products Confirmed Not Vulnerable, Details, Workarounds, Fixed Releases, Exploitation and Public Announcements	Final	2026-MAR-05

Show Complete History...

Legal Disclaimer

SOFTWARE DOWNLOADS AND TECHNICAL SUPPORT

The Cisco Support and Downloads page on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool. Please note that customers may download only software that was procured from Cisco directly or through a Cisco authorized reseller or partner and for which the license is still valid.

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco Technical Assistance Center (TAC). Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

When considering software upgrades, customers are advised to regularly consult the advisories for the relevant Cisco products to determine exposure and a complete upgrade solution. In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

LEGAL DISCLAIMER DETAILS

CISCO DOES NOT MAKE ANY EXPRESS OR IMPLIED GUARANTEES OR WARRANTIES OF ANY KIND, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, CISCO DOES NOT GUARANTEE THE ACCURACY OR COMPLETENESS OF THIS INFORMATION. THIS DOCUMENT IS PROVIDED ON AN " AS IS" BASIS. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Copies or summaries of the information contained in this Security Advisory may lack important information or contain factual errors. Customers are advised to visit the Cisco Security Advisories page for the most recent version of this Security Advisory. The Cisco Product Security Incident Response Team (PSIRT) assesses only the affected and fixed release information that is documented in this advisory. See the Cisco Security Vulnerability Policy for more information.

- Cisco Security Vulnerability Policy
- Subscribe to Cisco Security Notifications
- Related to This Advisory