Revision	Date	Changes
1.0	October 23, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-111943
CVSSv3.1 Base Score: Not yet available (see note below)
CVSSv4.0 Base Score: Not yet available (see note below)
Common Weakness Enumeration: CWE-299 Improper Check for Certificate Revocation
This vulnerability is being tracked by BUG 2045311(CVP), BUG 2045936(Wi-Fi AP), BUG 2045523(EOS), BUG 2045770(VeloCloud), BUG 2047171(DMF)

Note: Arista is not the CVE owner for this but estimates the score and vector as 9.2 / 10 (CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

Description

This security advisory is in response to the eMudhra Intermediate CA key compromise. This issue exposes affected systems to Man in the Middle (MitM) attacks. There are multiple CVEs tracking this issue. As of the time of this publication, CVE-2026-111943 is the only CVE, applicable to components used in Arista software products. This vulnerability applies to any software that verifies an X.509 certificate using a trust store that implicitly trusts any of the compromised CA certificates.

More information about the specific events that led to this CVE and this advisory can be found on this public web page: https://emudhra.we-have-a-problem.com/

Arista Engineering and PSIRT teams are comprehensively reviewing all product lines to identify the products that may be affected by this vulnerability. Arista will continue to update this advisory with possible mitigations and fixed software releases as soon as they are available.

Vulnerability Assessment

Platform and Software Applicability Note

To determine actual exposure, operators should first check their software versions against the "Affected Software" list below. If your software release is not listed, your deployment is not vulnerable, regardless of the hardware platform in use.

Affected Software

EOS Versions

- 4.36.3M and below releases in the 4.36.x train
- 4.35.7M and below releases in the 4.35.x train
- 4.34.9M and below releases in the 4.34.x train

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

- 4.33.11M and below releases in the 4.33.x train
- All releases in the 4.32.x train
- All releases in the 4.31.x train
- All releases in the 4.30.x train
- All releases in the 4.29.x train
- 4.28.14M and below releases in the 4.28.x train
- All releases in all trains prior to 4.28

Streaming Telemetry Agent (TerminAttr) Versions:

- v1.46.2 and below releases in the v1.46 train
- All releases in the v1.45 train
- All releases in the v1.44 train
- v1.43.10 and below releases in the v1.43 train
- All releases in the v1.42 train
- All releases in the v1.41 train
- v1.40.14 and below releases in the v1.40 train
- All releases in the v1.39 train
- All releases in the v1.38 train
- v1.37.14 and below releases in the v1.37 train
- All releases in the v1.36 train
- All releases in the v1.35 train
- v1.34.14 and below releases in the v1.34 train
- All releases in the v1.33 train
- All releases in the v1.32 train
- v1.31.17 and below releases in the v1.31 train
- All releases in all trains prior to v1.31

CloudVision Portal on-premises, virtual appliance or physical appliance (including the CV-CUE on premises software)

- 2026.3.0.1 and below releases in the 2026.3.x train
- 2026.2.2 and below releases in the 2026.2.x train
- 2026.1.4 and below releases in the 2026.1.x train
- All releases in all trains prior to 2026.1.x

CloudVision Appliance Versions

- 7.2.0 and below releases in the 7.2.x train
- 7.1.1 and below releases in the 7.1.x train
- 7.0.1 and below releases in the 7.0.x train
- All releases in all trains prior to 7.0.x

CloudVision Sensor Versions

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

- 1.4.3 and below releases in the 1.4.3 train
- All releases in all trains prior to 1.4

WIFI AP Versions

All releases are impacted including:

- 21.6.0M -8 and below releases in 21.X train
- 22.1.3F and below releases in 22.1.X train
- 22.3.0F-18 and below releases in 22.3.X train
- All releases in all trains prior to 21.X

DANZ Monitoring Fabric (DMF) Versions

- 8.10.1 and below releases in the 8.10.x train
- 8.9.1 and below releases in the 8.9.x train
- 8.8.1 and below releases in the 8.8.x train
- 8.7.3 and below releases in the 8.7.x train
- 8.6.3 and below releases in the 8.6.x train
- All releases in all trains prior to 8.5.x

Converged Cloud Fabric (CCF) Versions

- 6.2.5 and below releases in the 6.2.x train
- All releases in all trains prior to 6.2.x

CloudVision AGNI - Virtual or Physical Appliance

- P-2026.3.0 and below releases in 2026.3.X train
- P-2026.2.0 and below releases in 2026.2.X train
- P-2025.2.2 and below releases in 2025.2.X train
- P-2024.4.1 and below releases in 2024.4.X train

VeloCloud Edge Versions

- 7.0.0.0 (20260630) and below in the 7.0.0 train
- 6.4.4.0 (20260929) and below in the 6.4.4 train
- 6.2.0.1 (20250513) and below in the 6.2.0 train
- 6.1.6.0 (20260917) and below in the 6.1.6 train
- 5.2.7.0 (20260712) and below in the 5.2.7 train

VeloCloud Gateway Versions

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

- 7.0.0.0 (20260630) and below in the 7.0.0 train
- 6.4.4.0 (20260929) and below in the 6.4.4 train
- 6.2.0.1 (20250513) and below in the 6.2.0 train
- 6.1.6.0 (20260917) and below in the 6.1.6 train
- 5.2.7.0 (20260712) and below in the 5.2.7 train

VeloCloud Orchestrator Versions

- 6.4.2.12 and below releases in the 6.4.2 train
- 6.1.3.10 and below releases in the 6.1.3 train
- 5.2.3.18 and below releases in the 5.2.3 train

Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)

- NGFW 17.5.0 and prior

Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)

- All releases versioned as 5.2.0 and above and less than 5.4.12

Affected Platforms

The following products **are** affected by this vulnerability:

- Arista EOS-based products:
  - 710 Series
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series
  - 7010TX Series
  - 7020R/R4 Series
  - 7130 Series running EOS
  - 7170 Series
  - 7050X3/X4 Series
  - 7060X/X2/X4/X5/X6 Series
  - 7260X/X3 Series
  - 7280R/R2/R3/R4 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Serie

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

    - 7500R/R2/R3 Series
    - 7800R3/R4 Series
    - 7700R4 Series
    - AWE 5000 Series
    - AWE 7200R Series
    - ZTX-7200 Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
- Wi-Fi Access Points
- CloudVision Portal on-premises, virtual appliance or physical appliance (including the CV-CUE on premises software)
- CloudVision Sensor
- CloudVision Appliance Software
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- DANZ Monitoring Fabric (DMF) - Controller Appliance
- DANZ Monitoring Fabric (DMF) - Analytics Node Appliance
- DANZ Monitoring Fabric (DMF) - Recorder Node Appliance
- DANZ Monitoring Fabric (DMF) - Service Node Appliance
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
    - NDR nucleus
    - NDR sensors (the ava switch sensor is deployed inside of EOS)
    - NDR analyst portal
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)
- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

The following product versions and platforms **are not** affected by this vulnerability:

- Arista EOS-based products:
    - CloudVision eXchange, virtual or physical appliance
- CloudVision as-a-Service
- CloudVision CUE cloud service delivery

The following product versions and platforms are **undergoing triage** to determine if they are affected by this vulnerability:

- Arista 7130 Systems running MOS
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)
- Arista Multi Cloud Director (formerly Big Switch MCD)

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

Required Configuration for Exploitation

EOS

Features which establish an outgoing TLS connection from the EOS switch to external servers are at risk for being impacted by this vulnerability. Select features are assessed below. Other features are being evaluated and will be updated over time.

The following EOS features establish an outgoing TLS connection and are known **to be** impacted:

- Streaming Telemetry Agent (TerminAttr): TerminAttr, when used to establish a connection to CVaaS, is impacted by this issue if no CA root of trust is specified.
    - This is specified as the second argument to either certs or token-secure in the cvauth parameter when TerminAttr is configured.
    - Example **impacted** configuration parameters which are colored in red in the below example**:**
        - -cvauth=token-secure,/mnt/flash/token.json
        - -cvauth=certs,/mnt/flash/cert.pem,/mnt/flash/key.pem

```
switch> show running-configuration | section TerminAttr
daemon TerminAttr
   exec /usr/bin/TerminAttr -cvaddr=apiserver.arista.io:443 -cvcompression=gzip -cvvr
f=management -taillogs
-cvauth=token-secure,/mnt/flash/token.json
   no shutdown
```

```
switch> show running-configuration | section TerminAttr
daemon TerminAttr
   exec /usr/bin/TerminAttr -cvaddr=apiserver.arista.io:443 -cvcompression=gzip -cvvr
f=management -taillogs
-cvauth=certs,/mnt/flash/cert.pem,/mnt/flash/key.pem
   no shutdown
```

Examples above show **impacted** configuration colored in red

- Example **non impacted** configuration parameters with the additional root of trust highlighted in yellow:
- -cvauth=token-secure,/mnt/flash/token.json,/mnt/flash/ca.pem
- -cvauth=certs,/mnt/flash/cert.pem,/mnt/flash/key.pem,/mnt/flash/ca.pem

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
switch> show running-configuration | section TerminAttr
daemon TerminAttr
   exec /usr/bin/TerminAttr -cvaddr=apiserver.arista.io:443 -cvcompression=gzip -cvvr
f=management -taillogs
-cvauth=token-secure,/mnt/flash/token.json,/mnt/flash/ca.pem
   no shutdown
```

```
switch> show running-configuration | section TerminAttr
daemon TerminAttr
   exec /usr/bin/TerminAttr -cvaddr=apiserver.arista.io:443 -cvcompression=gzip -cvvr
f=management -taillogs
-cvauth=certs,/mnt/flash/cert.pem,/mnt/flash/key.pem,/mnt/flash/ca.pem
   no shutdown
```

Examples above show the configuration which makes this **non impacting** highlighted in yellow

- In addition custom scripting which uses utilities included in EOS such as curl and wget will be impacted by this unless those utilities are specifically configured to not use the default EOS trust bundle.

The following EOS features establish an outgoing TLS connection and are known to **not be** impacted:

- CLI “copy” command - this command does not verify remote peers so there is no impact here.
- OpenConfig
- CloudVision Exchange / Media Control Services (MCS)
- TACACS+ over TLS
- RADsec (RADIUS over TLS)
- Syslog over TLS
- STUN
- Automatic Certificate Management (implementing RFC 7030 compliant EST)
- SensorClient
- NTS (NTP over TLS)

CloudVision Portal

Features which establish an outgoing TLS connection from the CloudVision Portal to external servers are at risk for being impacted by this vulnerability. Select features are assessed below. Other features are being evaluated and will be updated over time.

The following features are known **to be** impacted:

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

- Authentication and certificate services:
  - LDAPS
  - RADIUS over TLS (RadSec)
  - HTTPS requests to OIDC identity providers and SAML metadata endpoints
  - External certificate-management services such as Venafi
- Downloads and Arista services:
  - Image Repository Image Upload and Download, when CloudVision reaches out to the arista.com software downloads site
  - Compliance Dashboard, when CloudVision reaches out to the arista.com AlertBase for updates for bug-advisory retrieval and validation
- Notifications and data exports:
  - HTTPS webhooks
  - Alerter
  - syslog over TLS
- Sensor and data-source integrations: TLS connections to configured external and 3rd party systems including but not limited to:
  - CloudVision AGNI
  - MSS integrations, including Palo Alto Networks, CMDB/IPAM, etc
  - DANZ Monitoring Fabric (DMF)
  - F5 BIG-IP
  - OpenStack
  - VMware vCenter
  - Cisco ISE
  - HPE ClearPass
  - ServiceNow
  - Bizzdesign
  - Helix integrations
  - Other outgoing sensor and data-source integrations
- Script Executor
  - Customer scripts and utilities: Outbound HTTPS or other TLS connections made by scripts that use the system provided trust store.

CV Sensor

Specific impacted features are being evaluated at this time.

CV-CUE

Specific impacted features are being evaluated at this time.

WiFi Access Points

The following features are known **to be** impacted:

- Connections from the AP to the CV-CUE controller

No other features are impacted.

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

DMF, CCF, and CloudVision Appliance Software (CVA)

Features which establish an outgoing TLS connection from DMF, CCF, or CVA to external servers and which use the public CA trust bundle are at risk for being impacted by this vulnerability. The features listed below have to be manually triggered by an administrator. Note that features that require configuration of specific CA authorities (ex., Syslog over TLS) are not affected.

The following DMF, CCF, and CVA features establish an outgoing TLS connection and are known **to be** impacted:

- **Appliance image import or upgrade from HTTPS**, including copy https://… image://… and cluster image copy. Certificate verification is on by default. Image-signature checks remain a separate safeguard against unsigned installation.
- **HTTPS file and configuration imports:** copy https://… file://… and copy https://… running-config. The latter can apply downloaded configuration.
- **Admin snapshot fetch from HTTPS:** /snapshot/fetch verifies the server by default and stores the fetched snapshot. Applying a snapshot requires a separate action.
- **Support and diagnostics upload:** upload support and diagnose upload support verify the HTTPS control service and HTTPS bundle-upload destinations. The default control service is Diagus; automatic support upload is off unless enabled.

The following DMF and CVA feature establish an outgoing TLS connection and are known **to be** impacted:

- **CLI exports to HTTPS**, such as copying a file, configuration, snapshot, or support bundle to an HTTPS destination, and verifying the destination using public CA trust.

The following CCF features establish an outgoing TLS connection and are known **to be** impacted:

- copy https://… snapshot://… uses default certificate verification.
- install package https://…, backed by the admin copy-install action, downloads a .deb with default verification and then installs it.

The following CVA features establish an outgoing TLS connection and are known **to be** impacted:

- **Application package import:** copy https://… package://<name> verifies HTTPS by default. Package signature and checksum checks also default to enabled; the test rejected an unsigned package despite accepting the forged HTTPS peer.
- **Provisioning userdata import:** copy https://… userdata://<name> verifies HTTPS by default.

CloudVision AGNI - Virtual or physical appliance

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

Specific impacted features are being evaluated at this time.

VeloCloud Edge

- Management connections to the VeloCloud Orchestrator
- Download services for Advanced Thread Protection

VeloCloud Gateway

- Management connections to the VeloCloud Orchestrator

VeloCloud Orchestrator

Specific impacted features are being evaluated at this time.

Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)

Specific impacted features are being evaluated at this time.

Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)

Specific impacted features are being evaluated at this time.

Indicators of Compromise

There are no known reliable indicators of compromise for this vulnerability. Please contact support if there are any questions or if any suspicious behavior is identified.

Mitigation

EOS

The recommendation is to ultimately upgrade to the latest version of EOS with a fix as soon as it is available.

If any custom scripts have been deployed on EOS that initiate outbound connections (using, for example, curl, wget, Python urllib, Go net/http, and possibly others) to anywhere beyond trusted network boundaries, these still remain vulnerable in the meantime. In this case, as a stop-gap measure to untrust the compromised CA certificates, the following shell commands can be run with superuser privileges.

The below mitigation script only needs to be run if custom scripts or programs which use the default trust store are running on an EOS device. This is not a normal scenario.

```
switch> enable
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
switch# bash

Arista Networks EOS shell

[admin@switch ~]$ sudo su
bash-5.1# d=/etc/pki/ca-trust/source/blocklist; [ -d $d ] || d=/etc/pki/ca-
trust/source/blacklist
trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=Comodo%20AAA%20Services%20root;type=cert' \
  $d/Comodo_AAA_Services_root.pem &&
openssl x509 -in $d/Comodo_AAA_Services_root.pem \
  -out $d/Comodo_AAA_Services_root.pem \
  -trustout -addreject anyExtendedKeyUsage &&
trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20G3;type=cert' \
  $d/emSign_ECC_Root_CA_-_G3.pem &&
openssl x509 -in $d/emSign_ECC_Root_CA_-_G3.pem \
  -out $d/emSign_ECC_Root_CA_-_G3.pem \
  -trustout -addreject anyExtendedKeyUsage &&
update-ca-trust && echo "ok"
ok
```

The above script in **bold** should be run as a single command on the bash shell from superuser mode. It will echo “ok” at the end if successful.

Then verify that the two PEM files are present in the **/etc/pki/ca-trust/source/blocklist/** directory:

```
bash-5.1# ls -lh /etc/pki/ca-trust/source/blocklist/
total 8.0K
-r--r--r-- 1 root root 1.6K Jan  1 12:00 Comodo_AAA_Services_root.pem
-r--r--r-- 1 root root  891 Jan  1 12:00 emSign_ECC_Root_CA_-_G3.pem
```

The above shows a directory listing showing the CA certificates added to the “blocklist”.

Note that this series of commands needs to be run after every switch reboot until a version of EOS with a permanent fix has been installed.

WARNING: While the risk is low that the reachability to legitimate non-Arista TLS endpoints may be negatively impacted by this mitigation, some risk nevertheless remains. Employing this mitigation may result in failing TLS handshakes for connections where there is still a reliance on a verification path anchored at one of these root CA certificates. If it is determined that such a

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

compromise is not acceptable, then this mitigation can be undone by simply removing the PEM files from the **blocklist** directory (as shown above) and running **update-ca-trust** with superuser privileges.

Streaming Telemetry Agent (TerminAttr)

Streaming Telemetry Agent (TerminAttr) can accept specified trust bundles instead of relying on the default system trust bundle. This can be used to connect to CloudVision on-premise or CVaaS by specifying the root of trust for those endpoints. CloudVision on-premise roots of trust are defined by the server certificate the operator configures, whereas for CVaaS the roots of trust can be found at https://github.com/cloudflare/cfssl_trust/blob/master/ca-bundle.crt

To configure a specific trust bundle, save the certificate(s) in a file on the filesystem, such as /mnt/flash/ca.pem. The file should be in PEM format, with multiple certs appended with a newline delimiter. See the roots of trust for CVaaS for an example of this. The roots of trust are then specified as an additional argument in the “-cvauth” parameter.

A method to configure this for CVaaS is shown below. This starts by copying the roots of trust to /mnt/flash/ca.pem. From there depending on how TerminAttr is configured it will need to be adjusted to pass in the additional parameter.

```
switch> copy
https://raw.githubusercontent.com/cloudflare/cfssl_trust/refs/heads/master/ca-
bundle.crt flash:ca.pem
```

Example showing copying the roots of trust for CVaaS to /mnt/flash/ca.pem

Next TerminAttr needs to be configured to use the CA file. This involves adding an additional parameter to the `**-cvauth**` option to refer to the CA file. Depending on how TerminAttr is configured a couple possible ways to do so are shown below in yellow, where the original configuration which gets changed is shown in red:

```
switch>enable
switch#configure
switch(config)# daemon TerminAttr
switch(config-daemon-TerminAttr)#show active
   exec /usr/bin/TerminAttr -cvaddr=apiserver.arista.io:443 -cvcompression=gzip -cvvr
f=management -taillogs -cvauth=token-secure,/tmp/cv-onboarding-token
switch(config-daemon-TerminAttr)# exec /usr/bin/TerminAttr -cvaddr=apiserver.arista.i
o:443 -cvcompression=gzip -cvvrf=management -taillogs -cvauth=token-secure,/tmp/cv-
onboarding-token,/mnt/flash/ca.pem
switch(config-daemon-TerminAttr)# shutdown
switch(config-daemon-TerminAttr)# wait-for-warmup
switch(config-daemon-TerminAttr)# no shutdown
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

Example showing how to configure the CA root of trust when -cvauth is using token-secure. The additional parameter is highlighted in yellow.

```
switch>enable
switch#configure
switch(config)# daemon TerminAttr
switch(config-daemon-TerminAttr)#show active
   exec /usr/bin/TerminAttr -cvaddr=apiserver.arista.io:443 -cvcompression=gzip -cvvr
f=management -taillogs -cvauth=certs,/mnt/flash/cert.pem,/mnt/flash/key.pem
switch(config-daemon-TerminAttr)# exec /usr/bin/TerminAttr -cvaddr=apiserver.arista.i
o:443 -cvcompression=gzip -cvvrf=management -taillogs -cvauth=certs,/mnt/flash/cert.p
em,/mnt/flash/key.pem,/mnt/flash/ca.pem
switch(config-daemon-TerminAttr)# shutdown
switch(config-daemon-TerminAttr)# wait-for-warmup
switch(config-daemon-TerminAttr)# no shutdown
```

Example showing how to configure the CA root of trust when -cvauth is using certs. The additional parameter is highlighted in yellow.

Once the “exec” command is changed the next set of commands for “shutdown”, “wait-for-warmup”, “no shutdown” ensure that the TerminAttr daemon is restarted with the correct configuration.

CloudVision Portal

Solutions are being investigated and this section will be updated once available.

CloudVision Sensor

Solutions are being investigated and this section will be updated once available.

CV-CUE

Solutions are being investigated and this section will be updated once available.

WiFi Access Points

No mitigations are available. Please upgrade to a fixed release when possible.

DMF, CVA

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

The following mitigation applies to DMF version 8.7.0 and above, or CVA version 7.0.0 and above:

Given limited exposure of this issue in DMF/CVA features, we recommend users upgrade to a fixed release when possible.

Optionally, the script below can be used to block the affected CA certificates. The script needs to be run as root (sudo <filename>), from bash (debug bash), by an administrator or the recovery user.

```
#!/usr/bin/env bash
# Temporarily distrust the two roots named in RHSB-2026-012 on AlmaLinux 9.
set -euo pipefail

readonly COMODO_FILTER='pkcs11:object=Comodo%20AAA%20Services%20root;type=cert'
readonly
 COMODO_SHA256='D7A7A0FB5D7E2731D771E9484EBCDEF71D5F0C3E0A2948782BC83EE0EA699EF4'
readonly EMSIGN_FILTER='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20G3;type=cert'
readonly
 EMSIGN_SHA256='86A1ECBA089C4A8D3BBE2734C612BA341D813E043CF9E8A862CD5C57A36BBE6B'

die() {
  printf 'Error: %s\n' "$*" >&
  exit
}

verify_certificate() {
  local name=$
  local expected_sha256=$
  local certificate=$
  local fingerprint
  local canonical=$work_dir/canonical.pem

  [[ -s $certificate ]] || die "$name: certificate file is empty"
  openssl x509 -in "$certificate" -outform PEM -out "$canonical" ||
    die "$name: invalid PEM certificate"
  cmp -s -- "$certificate" "$canonical" ||
    die "$name: expected exactly one canonical PEM certificate"

  fingerprint=$(openssl x509 -in "$certificate" -noout -fingerprint -sha256)
  fingerprint=$
  fingerprint=$
  [[ $fingerprint == "$expected_sha256" ]] || die "$name: unexpected SHA-256 fingerpr
int: $fingerprint"
}
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
verify_permissions() {
  local certificate=$1
  local owner_group_mode

  owner_group_mode=$(stat -c '%u:%g:%a' -- "$certificate")
  [[ $owner_group_mode == 0:0:644 ]] ||
    die "$certificate must be root:root with mode 0644 (found $owner_group_mode)"
}

prepare_certificate() {
  local name=$
  local filter=$
  local expected_sha256=$
  local destination=$
  local extracted=$

  [[ ! -L $destination ]] || die "$destination is a symlink; review it manually"
  if [[ -e $destination ]]; then
    [[ -f $destination ]] || die "$destination is not a regular file; review it manua
lly"
    verify_certificate "$name" "$expected_sha256" "$destination"
    verify_permissions "$destination"
  else
    trust extract --format=pem-bundle --filter="$filter" "$extracted"
    verify_certificate "$name" "$expected_sha256" "$extracted"
  fi
}

install_and_verify() {
  local name=$
  local expected_sha256=$
  local extracted=$
  local destination=$

  [[ ! -L $destination ]] || die "$destination is a symlink; review it manually"
  if [[ ! -e $destination ]];  then
    install -o root -g root -m  0644 -- "$extracted" "$destination" ||
      die "Could not install $destination; inspect and remove any partial file before
 rerunning"
  fi
  [[ ! -L $destination && -f $destination ]] || die "$destination is not a regular fi
le; review it manually"
  verify_certificate "$name" "$expected_sha256" "$destination"
  verify_permissions "$destination"
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
}

[[ $ # == 0 ]] || die "Usage: $0"
(( EUID ==   )) || die 'Run this script as root'

blocklist_dir=/etc/pki/ca-trust/source/blocklist
[[ -d $blocklist_dir ]] || die "$blocklist_dir does not exist"
# Hold the directory lock through update-ca-trust so overlapping runs cannot
# replace a certificate while another run regenerates the trust stores.
exec <"$blocklist_dir" || die "Could not open $blocklist_dir for locking"
flock -x -w 60
 "$blocklist_lock_fd" || die 'Could not acquire the blocklist lock within 60 seconds'

comodo_dest=$blocklist_dir/Comodo_AAA_Services_root.pem
emsign_dest=$blocklist_dir/emSign_ECC_Root_CA_-_G3.pem

work_dir=$(mktemp -d)
trap 'rm -rf -- "$work_dir"' EXIT

comodo_pem=$work_dir/comodo.pem
emsign_pem=$work_dir/emsign.pem
# Check both roots before writing either blocklist file. Matching files also
# make an interrupted installation or trust refresh safe to retry.
prepare_certificate 'Comodo AAA Services root' \
  "$COMODO_FILTER" "$COMODO_SHA256" \
  "$comodo_dest" "$comodo_pem"
prepare_certificate 'emSign ECC Root CA - G3' \
  "$EMSIGN_FILTER" "$EMSIGN_SHA256" \
  "$emsign_dest" "$emsign_pem"

install_and_verify 'Comodo AAA Services root' "$COMODO_SHA256" "$comodo_pem" "$comodo
_dest"
install_and_verify 'emSign ECC Root CA - G3' "$EMSIGN_SHA256" "$emsign_pem" "$emsign_
dest"
update-ca-trust || die 'update-ca-
trust failed; blocklist files remain. Fix the cause and rerun this script'
printf 'Installed both RHSB-2026-012 blocklist files and ran update-ca-trust.\n'
printf 'Restart long-running TLS clients and verify forged-chain rejection.\n'
```

AGNI On-Premises

No mitigations are available. Please upgrade to a fixed release when possible.

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

VeloCloud Edge

With this vulnerability, Edge communications to the VCO could be susceptible to a man-in-the-middle attack, in which an attacker impersonates the VCO on the Edge's management connection. Edge data-plane tunnels and VCO-issued device certificates are not affected.

Interim Host Mitigation

Until the Edge is upgraded to a fixed release, the following script can be used to remove the root CAs validating the compromised certificates. Connections to a VeloCloud VCO will not be impacted.

```
#!/bin/sh
set -eu

CERT_DIR=/etc/ssl/certs
BUNDLE="$CERT_DIR/ca-certificates.crt"
MGD_CA_DIR=/etc/vc-public
MGD_CA="$MGD_CA_DIR/default_public_ca.certs"
BUNDLE_BACKUP="$BUNDLE.bak"
TMP_BUNDLE="$CERT_DIR/.ca-certificates.crt.tmp.$$"
TMP_MGD_CA="$MGD_CA_DIR/.default_public_ca.certs.tmp.$$"
TMP_TEST_BODY="$MGD_CA_DIR/.edge-ca-patch-response.$$"

# CA certificate basenames to remove from CERT_DIR.
CA_CERTS='
Comodo_AAA_Services_root.crt
emSign_ECC_Root_CA_-_G3.crt
'

# HTTPS test URLs from the incident site's checker.js.
TEST_URLS='
https://dv-g3b-emudhra.we-have-a-problem.com/
https://dv-g3c-emudhra.we-have-a-problem.com/
https://ov-g3b-emudhra.we-have-a-problem.com/
https://ov-g3c-emudhra.we-have-a-problem.com/
https://ev-g3b-emudhra.we-have-a-problem.com/
https://ev-g3c-emudhra.we-have-a-problem.com/
https://dv-g3b-aaa-emudhra.we-have-a-problem.com/
https://dv-g3c-aaa-emudhra.we-have-a-problem.com/
https://ov-g3b-aaa-emudhra.we-have-a-problem.com/
https://ov-g3c-aaa-emudhra.we-have-a-problem.com/
https://ev-g3b-aaa-emudhra.we-have-a-problem.com/
https://ev-g3c-aaa-emudhra.we-have-a-problem.com/
https://dv-g3b-noct-emudhra.we-have-a-problem.com/
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
https://dv-g3b-aaa-noct-emudhra.we-have-a-problem.com/
'
EXPECTED_BODY='Your client successfully connected to the site.'
RUN_URL_TESTS=0

case $# in
    0)
        ;;
    1)
        if [ "$1" = "--test" ]; then
            RUN_URL_TESTS=1
        else
            echo "Usage: $0 [--test]" >&2
            exit 2
        fi
        ;;
    *)
        echo "Usage: $0 [--test]" >&2
        exit 2
        ;;
esac

cleanup() {
    rm -f "$TMP_BUNDLE" "$TMP_MGD_CA" "$TMP_TEST_BODY"
}
trap cleanup 0
trap 'exit 1' 1 2 15

if [ ! -d "$CERT_DIR" ]; then
    echo "Certificate directory not found: $CERT_DIR" >&2
    exit 1
fi
if [ ! -f "$BUNDLE" ]; then
    echo "CA bundle not found: $BUNDLE" >&2
    exit 1
fi
if [ "$RUN_URL_TESTS" -eq 1 ] && ! command -v curl >/dev/null 2>&1; then
    echo "curl is required to verify the compromised-CA test URLs" >&2
    exit 1
fi

mkdir -p "$MGD_CA_DIR"
if [ ! -e "$BUNDLE_BACKUP" ]; then
    cp -p "$BUNDLE" "$BUNDLE_BACKUP"
fi
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
# Prune certs
certs_modified=0
for name in $CA_CERTS; do
    cert="$CERT_DIR/$name"
    for link in "$CERT_DIR"/*; do
        [ -L "$link" ] || continue
        if target=$(readlink "$link" 2>/dev/null) &&
           [ "$" = "$name" ]; then
            rm -f "$link"
            certs_modified=1
        fi
    done

    if [ -f "$cert" ] || [ -L "$cert" ]; then
        echo "Removing $name"
        rm -f "$cert"
        certs_modified=1
    fi
done

# Rebuild consolidated CA bundle
: > "$TMP_BUNDLE"
for cert in "$CERT_DIR"/*.crt; do
    [ -f "$cert" ] || continue
    [ "$cert" = "$BUNDLE" ] && continue
    cat "$cert" >> "$TMP_BUNDLE"
    printf '\n' >> "$TMP_BUNDLE"
done
if [ ! -s "$TMP_BUNDLE" ]; then
    echo "No individual CA certificates found in $CERT_DIR" >&2
    exit 1
fi

# Update mgd CA cache
: > "$TMP_MGD_CA"
for cert in "$CERT_DIR"/*.crt; do
    [ -f "$cert" ] || continue
    if [ "$cert" = "$BUNDLE" ]; then
        cat "$TMP_BUNDLE" >> "$TMP_MGD_CA"
    else
        cat "$cert" >> "$TMP_MGD_CA"
    fi
done
if [ ! -s "$TMP_MGD_CA" ]; then
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
    echo "No CA certificates available for MGD in $CERT_DIR" >&2
    exit 1
fi

chmod 644 "$TMP_BUNDLE" "$TMP_MGD_CA"
if ! cmp -s "$TMP_BUNDLE" "$BUNDLE"; then
    mv -f "$TMP_BUNDLE" "$BUNDLE"
    certs_modified=1
fi
if ! cmp -s "$TMP_MGD_CA" "$MGD_CA"; then
    mv -f "$TMP_MGD_CA" "$MGD_CA"
    certs_modified=1
fi

# Restart mgd if certs changed
if [ "$certs_modified" -eq 1 ]; then
    echo "Restarting mgd to reload the CA certificates"
    pkill -x mgd || true
fi

echo "Updated $BUNDLE and $MGD_CA"

if [ "$RUN_URL_TESTS" -eq 0 ]; then
    echo "Skipping URL checks; rerun with --test to verify the compromised-
CA endpoints"
    exit 0
fi

probe_failed=0
probe_inconclusive=0

for url in $TEST_URLS; do
    if curl --noproxy '*' --silent --show-error \
        --connect-timeout 5 --max-time 10 \
        --cacert "$MGD_CA" --output "$TMP_TEST_BODY" "$url"; then
        if grep -Fq "$EXPECTED_BODY" "$TMP_TEST_BODY"; then
            echo "FAIL: compromised chain was trusted: $url" >&2
            probe_failed=1
        else
            echo "INCONCLUSIVE: connected, but response body did not match: $url" >&2
            probe_inconclusive=1
        fi
    else
        curl_status=$?
        if [ "$curl_status" -eq 60 ]; then
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
            echo "PASS: certificate verification rejected the chain: $url"
        else
            echo "INCONCLUSIVE: curl exited $curl_status for $url" >&2
            probe_inconclusive=1
        fi
    fi
done

if [ "$probe_failed" -eq 1 ]; then
    echo "One or more compromised chains still validated against the MGD CA cache" >&
2
    exit 1
fi
if [ "$probe_inconclusive" -eq 1 ]; then
    echo "Some test URLs could not be conclusively checked; rerun when network access
 is available" >&2
    exit 2
fi

echo "All compromised-CA test URLs were rejected by the MGD CA cache"
```

VeloCloud Gateway

With this vulnerability, Gateway communications to the VCO could be susceptible to a man-in-the-middle attack, in which an attacker impersonates the VCO on the Gateway's management connection. Gateway data-plane tunnels and VCO-issued device certificates are not affected.

Interim Host Mitigation

Until the Gateway is upgraded to a fixed release, install the ca-certificates package at the version below or later for the Gateway's release. Executing the workaround will not impact dataplane traffic.

- Gateway 5.x (Ubuntu 18.04): 202402031ubuntu0.18.04.1+esm3 or later
- Gateway 6.x (Ubuntu 22.04): 20260816ubuntu0.22.04.1 or later
- Gateway 7.x (Ubuntu 24.04): 20260816ubuntu0.24.04.1 or later

Steps, as root:

```
# Detect: any output means the Gateway is affected
openssl crl2pkcs7 -nocrl -certfile /etc/vc-public/default_public_ca.certs |
 openssl pkcs7 -print_certs -noout |
 grep -E 'emSign ECC Root CA - G3|AAA Certificate Services'
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
# 1. Back up mgd's CA list
cp -p /etc/vc-public/default_public_ca.certs /root/default_public_ca.certs.bak

# 2. Install the fixed ca-certificates package (copied to /root)
dpkg -i /root/ca-certificates_<version>_all.deb

# 3. Rebuild mgd's CA list from the updated system list
cat /etc/ssl/certs/*.crt > /etc/vc-public/default_public_ca.certs

# 4. Restart mgd only (vc_procmon relaunches it)
kill -TERM $(pgrep -f '^/usr/bin/python3 /opt/vc/sbin/mgd$')

# Verify: package is at the fixed version or later
dpkg-query -W ca-certificates

# Verify: no output expected
openssl crl2pkcs7 -nocrl -certfile /etc/vc-public/default_public_ca.certs |
 openssl pkcs7 -print_certs -noout |
 grep -E 'emSign ECC Root CA - G3|AAA Certificate Services'

# Verify: the Gateway shows as Connected in the VCO

# 5. Once the Gateway is Connected, remove the backup and the downloaded package
rm -f /root/default_public_ca.certs.bak /root/ca-certificates_<version>_all.deb
```

VeloCloud Orchestrator

VCO device authentication using VCO-issued certificates and dedicated CA chains is not affected.

- **Hosted deployments:** We have verified that the deployed server certificate chains used for data plane-to-VCO and management plane communication do not include the affected intermediates.
- **On-prem deployments:** Check your server certificate chain using the command below to determine whether certificate replacement is required.
- **Outbound connections:** In both hosted and on-prem deployments, VCO can connect to customer-configured third-party services, including SSO providers. These connections have separate exposure through public CA trust, regardless of the VCO's own server certificate.

On-Prem Server Certificate Check

Replace vco.example.com with your VCO hostname. This command checks the presented chain for the eight published affected CA names:

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
VCO_HOST='vco.example.com'
openssl s_client -connect "$:443" -servername "$VCO_HOST" \
  -showcerts </dev/null >/dev/null |
  grep -E 'EM (DV TLS|OV TLS|EV TLS|OV CS) CA - G3[BC]'
```

If certificate lines appear, an affected CA name was found. Ask your certificate provider to confirm and replace affected server certificates.

This checks server CA names only; it does not validate certificates or assess VCO outbound client exposure.

Interim Host Mitigation

Upgrade to a fixed VCO release for full mitigation. Until then, the following Ubuntu host trust-store changes reduce exposure but do not fully mitigate all outbound connections.

Perform these steps in a maintenance window. Removing these roots may disrupt legitimate third-party integrations whose certificates rely on them. We recommend this temporary measure because continued trust can also allow fraudulent certificates issued using the compromised intermediate CA keys to be accepted.

Perform all steps on the active VCO and, in a DR configuration, on the standby VCO, one host at a time.

1. Back Up the Trust Configuration

This preserves an existing backup if the command is repeated. Stop if a command fails.

```
sudo cp -pn /etc/ca-certificates.conf /etc/ca-certificates.conf.pre-emudhra
```

2. Disable the Roots and Regenerate the Trust Store

The entries below correspond to **emSign ECC Root CA - G3** and **AAA Certificate Services**. The commands add to disable them, then rebuild the system trust store:

```
sudo sed -i \
  -e 's|^mozilla/emSign_ECC_Root_CA_-_G3.crt$|!&|' \
  -e 's|^mozilla/Comodo_AAA_Services_root.crt$|!&|' \
  /etc/ca-certificates.conf

sudo update-ca-certificates
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

One or both entries may be absent. Check /etc/ca-certificates.conf.pre-emudhra to see which were present before the change. Each entry that was present should now start with :

```
grep -E '^!?mozilla/(emSign_ECC_Root_CA_-_G3|Comodo_AAA_Services_root)\.crt$' \
  /etc/ca-certificates.conf
```

3. Restart and Verify Services

Validate nginx configuration first. Proceed only if this succeeds:

```
sudo nginx -t
```

Restart the services:

```
sudo systemctl restart nginx backend portal upload replication sdwan-api
sudo systemctl is-active nginx backend portal upload replication sdwan-api
```

Confirm the services are running, then verify VCO access, device connectivity, and configured integrations such as SSO and test email. Contact TAC for certificate errors; do not disable certificate verification or re-enable the removed roots to bypass them.

NDR

NDR has a hotfix that can be quickly deployed by operations staff to block the eMudhra CA chain, similar in principle to EOS. This would be durable past reboots too. To apply the necessary mitigation for this issue, please contact the Arista TAC team to remove eMudhra compromised CAs.

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience. Arista recommends customers move to the latest version of each release that contains all the fixes listed below.

The issue is fixed in the following product releases:

EOS

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

This section will be updated once fixed releases are available.

Streaming Telemetry Agent (TerminAttr)

- TerminAttr v1.43.11, which supports EOS 4.30.0F through 4.35.7M
- TerminAttr v1.46.3, which supports EOS 4.30.0F through 4.36.3M

Note: the Streaming Telemetry Agent upgrade alone provides remediation for the EOS to CloudVision connection. However, a full EOS upgrade is required to provide complete remediation from this issue, including cases where custom scripts or agents reach out to external entities. If no custom scripts or agents are used on the EOS device, then the Streaming Telemetry Agent alone provides a solution for complete remediation.

CloudVision Portal

This section will be updated once fixed releases are available.

CV Sensor

This section will be updated once fixed releases are available.

CV-CUE

This section will be updated once fixed releases are available.

WiFi Access Points

This section will be updated once fixed releases are available.

DMF

This section will be updated once fixed releases are available.

AGNI On-Premises

This section will be updated once fixed releases are available.

VeloCloud Edge

This section will be updated once fixed releases are available.

VeloCloud Orchestrator

- 6.4.2.13 and later releases in the 6.4.2 train
- 6.1.3.11 and later releases in the 6.1.3 train

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

- 5.2.3.19 and later releases in the 5.2.3 train

Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)

This section will be updated once fixed releases are available.

Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)

This section will be updated once fixed releases are available.

For More Information

If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

Open a Service Request

Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.