**Date: November 10, 2026**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | November 10, 2026 | Initial release |
| 1.1 | November 12, 2026 | Description clarification |

The CVE-ID tracking this issue: CVE-2026-121371
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
CVSSv4.0 Base Score: 8.7
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
This vulnerability is being tracked by BUG 2048764(EOS), BUG 2069205(DMF)

# Description

On affected EOS versions with the eAPI service enabled, a specially crafted HTTP request can allow an unauthenticated, remote attacker to read arbitrary files, including sensitive credentials from the switch filesystem. HTTPS, since it is HTTP over TLS, is also impacted by this issue.

This issue was discovered internally by Arista, and the company is not aware of any malicious exploitation of this vulnerability in customer networks.

# 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 earlier release in 4.36.x train
- 4.35.7M and earlier release in 4.35.x train
- 4.34.9M and earlier release in 4.34.x train
- 4.33.11M and earlier release in 4.33.x train
- All releases in the 4.32.x train
- All releases in the End of Support software release trains

### Impact on DANZ Monitoring Fabric (DMF)

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.

DANZ Monitoring Fabric (DMF) deploys a fixed version of Arista EOS on certain managed fabric switches. If the EOS version bundled with a DMF release falls within the affected version range of this advisory, DMF deployments using EOS-based switch platforms may be impacted.

DMF fabric switches running Switch Light OS are not affected by this vulnerability.

Customers running DMF should run the following command on the controller to identify the EOS version bundled with their deployment.

```
DMF-CONTROLLER> show version details
...
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ Platform files ~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
File
 Hcl supported Platform
--------------------------------------------------------------------------------------------
|-------------|-----------------------------------|
...
EOS-4.36.2F
-49446791.volgarel.1-x86_64.swi                                                  True
    x86_64-7289-eos
EOS-4.36.2F-49446791.volgarel.1-x86_64.swi
 True          i686-7289-eos
EOS-4.36.2F-49446791.volgarel.1-x86_64.swi
 False         x86_64-ccs-720df-48y-eos
```

## 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/XE7 Series
  - 7260X/X3 Series
  - 7280R/R2/R3/R4 Series

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.

  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7500R/R2/R3 Series
  - 7800R3/R4 Series
  - 7700R4 Series
  - AWE 5000 Series
  - AWE 7200R Series
  - ZTX-7200 Series
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - CloudVision eXchange, virtual or physical appliance

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

- Wi-Fi Access Points
- CloudVision CUE cloud service delivery
- CloudVision Portal on-premises, virtual appliance or physical appliance (including the CV-CUE on premises software)
- CloudVision Appliance Software
- CloudVision as-a-Service
- 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 Multi Cloud Director (formerly Big Switch MCD)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)
- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

## Required Configuration for Exploitation

In order to be vulnerable to CVE-2026-121371, the following conditions must all be met:

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.

- eAPI is enabled and running
- default-service is enabled

Note: The conditions listed above reflect default system configurations. As a result, systems remain vulnerable even without custom or explicit configuration changes.

To check if eAPI service is running, use the following command:

```
switch>show management api http-commands
Enabled: Yes
HTTPS server: running, set to use port 443
HTTP server: running, set to use port 80
Local HTTP server: shutdown, no authentication, set to use port 8080
Unix Socket server: shutdown, no authentication
VRFs: default
Hits: 0
Last hit: never
Bytes in: 0
Bytes out: 0
Requests: 0
Commands: 0
Duration: 0.0 seconds
SSL Profile: ARISTA_DEFAULT_SELF_SIGNED_PROFILE, valid
FIPS Mode: No
QoS DSCP: 0
Session Timeout: 1440 minutes
Log Level: none
CSP Frame Ancestor: None
TLS Protocols: 1.0 1.1 1.2 1.3
URLs
------------------------------------------------------------
Management1 : https://10.0.0.1:443
Management1 : http://10.0.0.1:80
Management1 : https://[3fff:ffff::1]:443
Management1 : http://[3fff:ffff::1]:80
```

To Verify if default-service is enabled by examining running-config all:

```
switch#show running-config all| sect http-server
management http-server
   protocol https port 443
   protocol http
   no protocol http localhost port 8080
```

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.

```
   no protocol unix-socket
   qos dscp 0
   no log-level
   default-services
   no header csp frame-ancestors
   no cors allowed-origin
   no protocol https ssl profile
```

Or

```
switch#show running-config all| sect http-commands
management api http-commands
   protocol https port 443
   no protocol http port 80
   no protocol http localhost port 8080
   no protocol unix-socket
   qos dscp 0
   no log-level
   default-services
   no header csp frame-ancestors
   ...
```

## Indicators of Compromise

Review local nginx access logs located at /var/log/nginx-access.log for irregular HTTP requests targeting device static resources, specifically focusing on requests constructed with unexpected paths.

## Mitigation

The recommended mitigation is to disable default services on the management HTTP server. Disabling the default services removes access to the built-in eAPI documentation/explorer (the web UI accessible to) and TapAgg GUI.

```
switch(config)#management http-server
switch(config-mgmt-http-server)#no default-services

switch#show running-config | sect http-server
management http-server
   no default-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.

Or

```
switch(config)#management api http-commands
switch(config-mgmt-api-http-cmds)#no default-services

switch#show running-config | sect http-commands
management api http-commands
   no default-services
   no shutdown
```

# 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. For more information about upgrading see EOS User Manual: Upgrades and Downgrades

CVE-2026-121371 has been fixed in the following releases:

- 4.37.0F and later release in 4.37.x train
- 4.36.3.2M and later releases in the 4.36.x train
- 4.35.7.2M and later releases in the 4.35.x train
- 4.34.9.2M and later releases in the 4.34.x train
- 4.33.11.2M and later releases in the 4.33.x train

## Hotfix

No hotfix available for this issue.

## 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
- By email: support@arista.com
- By telephone: List of regional telephone numbers

### Receive notification for new advisories and notices:

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.

Subscribeto the RSS feed and email notifications to receive periodic updates on new software releases, advisories, end of sale and field notices.

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.