Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-120976
CVSSv3.1 Base Score: 6.0 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N)
CVSSv4.0 Base Score: 7.0
(CVSS:4.0/AV:L/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-532: Insertion of Sensitive Information into Log File
This vulnerability is being tracked by BUG 1899357

Description

On affected platforms running Arista EOS with IEEE 802.1X authentication and MACsec using dynamically derived keys, sensitive authentication information may be recorded in diagnostic data during a Smart Switch Upgrade (SSU).

An attacker with administrative access on the device who obtains the affected diagnostic data could recover sensitive authentication information. This could potentially compromise the confidentiality and integrity of traffic protected by MACsec on the affected link.

The vulnerability is only exposed during and after an SSU reload where an active 802.1X session used for MACsec is present.

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

- Release 4.36.2F and below in the 4.36.x train
- Release 4.35.6M and below in the 4.35.x train
- Release 4.34.8M and below in the 4.34.x train
- Release 4.33.9M and below in the 4.33.x train
- All releases in the 4.32.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.

- End of Life software trains between 4.22.0F and 4.31 are also affected.

Affected Platforms

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

- Arista EOS-based products:
  - 7388-8D Series
  - 7500R/R2 Series
  - 7800/R3/R3A Series
  - 722XPM and 720XPM Series
  - 750X Series
  - 7050X3/X4 Series
  - 7170 Series
  - 7289R3 Series
  - 7500R3 Series
  - 7800R4 Series

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

- Arista EOS-based products:
  - 710 Series
  - 720D Series
  - 720XP Series
  - 7010TX Series
  - 7020R/R4 Series
  - 7130 Series running EOS
  - 7060X/X2/X4/X5/X6/XE7 Series
  - 7260X/X3 Series
  - 7280R/R2/R3/R3A/R4 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7700R4 Series
  - AWE 5000 Series
  - AWE 7200R Series
  - ZTX-7200 Series
  - CloudEOS
  - CloudVision eXchange, virtual or physical appliance
  - cEOS-lab
  - vEOS-lab
- Wi-Fi Access Points
- CloudVision CUE cloud service delivery

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.

- CloudVision Portal, 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-2026-120976, the following condition must be met:

For the MACsec key exposure described in this advisory, a device must meet **all** of these following configuration conditions:

1. IEEE 802.1X authentication is configured on the affected interface.
2. A MACsec profile containing key source dot1x is applied to **that same interface**, enabling MACsec to derive keys from successful 802.1X authentication.
   1.) 802.1X configuration

```
switch#show running-config section dot1x
dot1x system-auth-control
!
interface Ethernet1
   dot1x pae authenticator
   dot1x port-control auto
```

   2.) MACsec configuration

```
switch#show running-config section mac security
mac security
   profile macsecDot1xProfile
      key source dot1x
```

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.

```
!
interface Ethernet1
   mac security profile macsecDot1xProfile
```

Indicators of Compromise

There are no known indicators of compromise for this vulnerability.

Mitigation

There is no mitigation possible for this vulnerability.

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-2026-120976 has been fixed in the following releases:

- 4.37.0F and later releases in the 4.37.x train
- 4.36.3M and later releases in the 4.36.x train
- 4.35.7M and later releases in the 4.35.x train
- 4.34.9M and later releases in the 4.34.x train
- 4.33.10M and later releases in the 4.33.x train

Hotfix

There is no hotfix 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
- 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.