Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release
1.1	September 22, 2026	CSAF JSON file added
1.2	September 24, 2026	Update regarding the workaround for resolution and target release versions for DMF fixes
1.3	October 28, 2026	Updated vulnerability fixed release version and added hotfix SWIX patch for post-upgrade new SNMPv3 configuration issue

The CVE-ID tracking this issue: CVE-2026-73440
CVSSv3.1 Base Score: 4.2 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N)
CVSSv4.0 Base Score: 2.3
(CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer
This vulnerability is being tracked by BUG 1856462 (EOS), BUG 1987785 (EOS) and BUG 1966273 (DMF)

Description

On affected platforms running Arista EOS with Simple Network Management Protocol (SNMP) configured, SNMPv3 local or remote user credentials may be exposed as a one-way hashed, localized key value within the device's running and sanitized configurations. An authenticated user who gains access to this sensitive information could leverage it to perform unauthorized read operations on SNMP tables or to send fraudulent trap notifications to the Network Management System (NMS).

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

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.

vulnerable, regardless of the hardware platform in use.

Affected Software

EOS Versions

- 4.36.2F and below releases in the 4.36.x train
- 4.35.6M and below releases in the 4.35.x train
- 4.34.8M and below releases in the 4.34.x train
- 4.33.10M and below releases in the 4.33.x train
- All prior releases

Impact on DANZ Monitoring Fabric (DMF)

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
```

The above switches are running EOS 4.36.2F as shown in the first column

Affected Platforms

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 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
  - 7150 Series
  - 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 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, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision Appliance Software
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- DANZ Monitoring Fabric (DMF) - Controller 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.

- 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-2026-73440, the following conditions must all be met:

- SNMPv3 must be configured with at least one local or remote user that has an authentication key
- The SNMPv3 user CLI configuration uses the legacy syntax and does not include the updated **key <algo> <encrypted_text>** syntax as instructed in the Resolution section below.

SNMPv3 must be configured with at least one local or remote user that has an authentication key. For example:

```
switch# show running-config | section snmp-server
snmp-server user alice group_alice v3 localized f5717f2cdde9bb946d00
auth sha256
f4b9ec9a299a10a5dec3541f44f44000484254ee56fa404236730520e10ce689
```

To verify whether any SNMPv3 users with authentication are configured:

```
switch# show snmp user

User name      : alice
Security model : v3
Engine ID      : f5717f2cdde9bb946d00
Authentication : SHA-256
Privacy        : None
Group          : group_alice
```

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.

If SNMP is not configured or no SNMPv3 users are configured, there is no exposure to this issue and the **show snmp** output will look something like:

```
switch>show snmp
Chassis: XXXXXXXXXXX
SNMP agent enabled in VRFs: default
Transmit message maximum size: 65536
SNMP agent disabled:
 Either no communities and no users are configured, or no VRFs are configured.
```

Indicators of Compromise

No indicators of compromise exist.

Mitigation

No mitigation exists.

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.

Following the system upgrade, users are required to execute the syntax conversion command specified below to adopt the updated, encrypted SNMPv3 CLI format.

```
switch# configure convert new-syntax
```

The updated encrypted SNMPv3 CLI configuration follows this structure, incorporating the newly introduced **key <algo> <encrypted_text>** syntax:

```
switch# show running-config | grep snmp-server
snmp-server user alice group_alice v3 localized f5717f2cdde9bb946d00
auth sha256 key 7
005D110205085E520B754E1B591C504542585F557D2F217064607A10034752035500080755575640440F5
C00505053515F08525208035C1605525E0A040E781F4D
```

CVE-2026-73440 has been fixed in the following releases:

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.

- 4.36.3M 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
- 4.33.11M and later releases in the 4.33.x train

DANZ Monitoring Fabric (DMF)

The fixed EOS version addressing CVE-2026-73440 is bundled with the following DMF releases:

- 8.10.1 and later releases in the 8.10.x train
- 8.8.1 and later releases in the 8.8.x train

Hotfix

CVE-2026-73440 can be remediated using the hotfix detailed below. This hotfix is strictly applicable to the listed releases. All non-listed versions must be upgraded to a fixed release as specified above.

- 4.36.2F
- 4.35.6M
- 4.34.8M
- 4.33.10M

Post hotfix installation, users are required to execute the syntax conversion command to fix the malformed keys.

Note: Installing/uninstalling the SWIX will cause the ConfigAgent process to restart.

Version: 1.0
URL: SecurityAdvisory178_CVE-2026-73440_Hotfix.swix

```
SWIX hash:
8a11df104d6ada97f0d63ca87a6a03071524038af1f8cd4a0bbcba490ab80245c7b2cfb86be81c5e6773e
05801f3df098120f6053b130938230c79193386fe74
```

For instructions on installation and verification of the hotfix patch, refer to the “managing eos extensions” section in the EOS User Manual. Ensure that the patch is made persistent across reboots by running the command ‘**copy installed-extensions boot-extensions**’.

For More Information

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.

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.