Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-19641
CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
CVSSv4.0 Base Score: 6.9
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-116: Improper Encoding or Escaping
This vulnerability is being tracked by BUG 1595868, BUG 1966286 (DMF)

Description

On affected platforms running Arista EOS with password authentication configured, a specially crafted password can create orphan authentication sessions. Repeated exploitation of this issue can exhaust available authentication resources, resulting in legitimate users being unable to log in to the device.

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

- 4.36.0F and below releases in the 4.36.x train
- 4.35.5M and below releases in the 4.35.x train
- 4.34.7.1M and below releases in the 4.34.x train
- 4.33.8M 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
```

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
    - 7500R/R2/R3 Series
    - 7800R3/R4 Series
    - 7700R4 Series
    - AWE 5000 Series
    - AWE 7200R Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance

- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)

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
- 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)
- 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-2026-19641, both of the following conditions must be met:

1. Login authentication must be enabled, which is the default configuration.

The following command can be used to verify the login authentication methods.

```
switch>show aaa methods authentication
Authentication method lists for LOGIN:
  name=default methods=local
Authentication method list for ENABLE:
  name=default methods=local
Authentication method list for DOT1X:
  name=default methods=
```

If the “methods” under “Authentication method lists for LOGIN” does not show “none”, that means login authentication is enabled.

2. A service that accepts password-based authentication is enabled (e.g., SSH with password authentication, or telnet). By default, SSH with password authentication is enabled and telnet is disabled.
   For SSH, use the following command to check whether it is enabled for any VRF.

```
switch>show management ssh
User certificate authentication methods: none (neither trusted CA nor SSL prof
ile configured)
SSHD status for Default VRF: enabled
SSH connection limit: 50
SSH per host connection limit: 20
FIPS status: disabled
eAPI subsystem: enabled
```

Use the following command to check if password-based authentication is enabled for SSH. SSH is vulnerable if “password” or “keyboard-interactive” is listed.

```
switch>show run all section management ssh | grep protocol
   authentication protocol keyboard-interactive public-key
```

For Telnet, use the following command to check whether it is enabled for any VRF. Telnet is vulnerable if enabled.

```
switch>show management telnet
Telnet status for Default VRF is enabled
```

```
Telnet session limit is 20
Telnet session limit per host is 20
```

The device is vulnerable if login authentication is enabled and SSH with password-based method or Telnet is enabled.

Indicators of Compromise

EOS maintains an internal pool of pending authentication sessions with a limited capacity. Orphan sessions created by this vulnerability accumulate in this pool until it is full and blocks new logins.

The primary indicator of exploitation is the following syslog message, which indicates the authentication session pool has been exhausted:

```
switch>show logging | grep AAA_INCOMPLETE_LOGINS_LIMIT
%AAA-3-AAA_INCOMPLETE_LOGINS_LIMIT: Too many incomplete login attempts
```

Mitigation

The workaround is to disable password based authentication services, such as Telnet and SSH.

NOTE: This workaround only works for local authentication. There is no workaround if the device requires password authentication via a remote method, e.g. Terminal Access Controller Access-Control System Plus (TACACS+), Remote Authentication Dial In User Service (RADIUS) or Lightweight Directory Access Protocol (LDAP).

Use the following command to disable Telnet.

```
switch(config)#management telnet
switch(config-mgmt-telnet)#shutdown
```

On the client host, use the following command to generate SSH keys.

```
client# ssh-keygen -t ecdsa -b 521 -f testkey
```

Copy the SSH public key to the device and add it to the local user.

```
switch(config)#copy scp:<local_path_with_keys>/testkey.pub flash:
switch(config)#username <user> sshkey file flash:testkey.pub
```

Add public-key as the first protocol for SSH authentication, keep keyboard-interactive as the second protocol for now.

```
switch(config)#management ssh
switch(config)#authentication protocol public-key keyboard-interactive
```

Once you have verified that the user can know login without a password from the client host, remove keyboard-interactive from SSH authentication protocol configuration.

```
switch(config)#management ssh
switch(config)#authentication protocol public-key
```

WARNING: Incorrect configuration may block logins. Make sure public-key authentication works before removing keyboard-interactive from the configuration.

Instead of public key, certificate-based authentication can also be used as a workaround for local users.

Please find more details about how to configure certificate-based authentication in the SSH Certificates User Guide.

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-2026-19641 has been fixed in the following releases:

EOS Versions

- 4.36.1F and later releases in the 4.36.x train
- 4.35.6M and later releases in the 4.35.x train
- 4.34.8M and later releases in the 4.34.x train
- 4.33.9M and later releases in the 4.33.x train

Hotfix

No hotfix is 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

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