Date: July 22, 2025

Revision	Date	Changes
1.0	July 22, 2025	Initial release

The CVE-ID tracking this issue: CVE-2025-3456
CVSSv3.1 Base Score: 3.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N)
Common Weakness Enumeration: CWE-532: Insertion of Sensitive Information into Log File
This vulnerability is being tracked by BUG1114420

Description

On affected platforms running Arista EOS, the global common encryption key configuration may be logged in clear text, in local or remote accounting logs. Knowledge of both the encryption key and protocol specific encrypted secrets from the device running-config could then be used to obtain protocol specific passwords in cases where symmetric passwords are required between devices with neighbor protocol relationships.

Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.34.0F
- 4.33.3F and below releases in the 4.33.x train
- 4.32.5M and below releases in the 4.32.x train
- 4.31.7M and below releases in the 4.31.x train
- 4.30.10M and below releases in the 4.30.x train
- 4.29.10M and below releases in the 4.29.x train

Affected Platforms

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

- Arista EOS-based products:
  - 710 Series
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series

Copyright 2025 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.

- 7010 Series
- 7010X Series
- 7020R Series
- 7130 Series running EOS
- 7160 Series
- 7170 Series
- 7050X/X2/X3/X4 Series
- 7060X/X2/X4/X5/X6 Series
- 7250X Series
- 7260X/X3 Series
- 7280R/R2/R3 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
- CloudEOS
- cEOS-lab
- vEOS-lab
- CloudVision eXchange, virtual or physical appliance

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

- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)
- 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)

Required Configuration for Exploitation

Copyright 2025 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.

In order to be vulnerable to CVE-2025-3456, the following condition must be met:

The global custom encryption key must be configured:

```
switch#show running-config | sect management security
management security
   password encryption-key common custom <key>
```

Indicators of Compromise

No indicators of compromise exist.

Mitigation

There is no known mitigation for the issue. The recommended resolution is to upgrade to a remediated software version at your earliest convenience and afterwards rotate the custom global encryption-key.

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-2025-3456 has been fixed in the following releases:

- 4.34.1F and later releases in the 4.34.x train
- 4.33.4M and later releases in the 4.33.x train
- 4.32.6M and later releases in the 4.32.x train
- 4.31.8M and later releases in the 4.31.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:

Copyright 2025 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.

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 2025 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.