Date: November 2, 2026

Revision	Date	Changes
1.0	November 2, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-98432
CVSSv3.1 Base Score: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSSv4.0 Base Score: 9.2
(CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-416: Use After Free
This vulnerability is being tracked by BUG2039829 (EOS), BUG2063903 (CVA & DMF)

Description

Arista Networks is providing this security update in response to a vulnerability affecting the use of IPv4 in the Linux kernel. It is believed to be possible to allow an unauthenticated attacker remote code execution (RCE) in the kernel if exploited. As of the time of this publication the only known means of exploiting this vulnerability requires multipath TCP (MPTCP) to be enabled in the Linux kernel.

Because of the MPTCP prerequisite, few Arista product lines are affected, but the underlying issue is present in many products. This advisory is focused on products that are known to be impacted, with Mitigation and Remediation guidance provided for other products as a defense in depth.

This issue is a publicly disclosed vulnerability in open source software, 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

For this security advisory affected software is listing versions of software where there is an impact to the customer. As of the publication of this advisory that means that MPTCP must be enabled at the kernel level.

Wi-Fi Access Points

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.

- Wifi Access Points using the Linux Kernel v6.6 are vulnerable to this issue. Exact versions are being determined and this advisory will be updated once known.

Arista Network Detection and Response (NDR) Security Platform

- All versions prior to and including 5.4.11

Affected Platforms

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

- Wi-Fi Access Points
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)

The following product versions and platforms **are not** affected by this vulnerability. Please note, at this point this is an assessment of required configuration for exploitation, ie MPTCP being enabled, not of the vulnerable ipv4 code being present. Products with vulnerable ipv4 code will have fixed releases over time:

- 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
  - ZTX-7200 Series
  - CloudEOS

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.

    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance
- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)
- CloudVision CUE cloud service delivery
- CloudVision Appliance Software
- CloudVision Portal, virtual appliance or physical appliance (including the CV-CUE on premises software)
- 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)
- CloudVision as-a-Service

The following product versions and platforms **are under triage** to determine if they are by this vulnerability:

- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- 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

Wi-Fi Access Points

Wi-Fi Access Points are susceptible to exploitation when run in OpenConfig mode. This exposure is limited to locations where an OpenConfig listener can be reached, which is typically the management plane.

Arista Network Detection and Response (NDR) Security Platform

NDR devices are vulnerable by default. It is not possible to configure this.

Indicators of Compromise

There are no clear indicators of compromise for this issue. Unusually high amounts of traffic containing IPv4 options or kernel crashes may indicate attempted exploitation of this issue across products.

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.

Mitigation

Wi-Fi Access Points

Mitigations for Wi-Fi Access Points are under investigation. This section will be updated as they become available.

Arista Network Detection and Response (NDR) Security Platform

NDR will be disabling MPTCP in all non air-gapped platforms. This action will be performed automatically by NDR SREs and no customer configuration is required.

Air-gapped systems will need to contact Arista support for assistance in applying the patches.

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.

This section will be updated once fixed releases are available for the underlying kernel issue or to disable MPTCP.

Hotfix

No hotfix is available for these issues.

For More Information:

If you require further assistance, or if you have any further questions regarding this notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

- Open a Service Request: https://arista.com
- By email: support@arista.com
- By telephone: +1-408-547-5502, +1-866-476-0000 - more

Receive Notifications

Subscribe to the RSS feed and email notifications to receive periodic updates on new software releases, end of sale, end of support 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.