Date: November 19, 2026

Revision	Date	Changes
1.0	November 19, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-114938

Description

This security advisory is in response to the “Java4Shell” vulnerability (CVE-2026-114938), which affects software that uses the base64 decoder running on certain versions of the Java runtime on x86-64 systems with AVX-512 VBMI extensions enabled.

Arista is not currently aware of any malicious exploitation of this vulnerability in its products.

Vulnerability Assessment

Platform and Software Applicability Note

Platforms known to be unaffected at this time, as well as those still undergoing assessment regarding the possible applicability of this vulnerability, are listed below.

Unaffected Platforms

The following product versions and platforms **are not** 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/XE7 Series
  - 7260X/X3 Series
  - 7280R/R2/R3/R4 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series

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.

    - 7500R/R2/R3 Series
    - 7800R3/R4 Series
    - 7700R4 Series
    - AWE 5000/7200R Series
    - ZTX-7200 Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance
- Wi-Fi Access Points
- CloudVision Sensor
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical 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)

Platforms Undergoing Triage

The following product versions and platforms are still **undergoing triage** to determine further details in regards to this vulnerability:

- CloudVision CUE cloud service delivery
- CloudVision Portal on-premises, virtual appliance or physical appliance (including the CV-CUE on premises software)
- CloudVision Appliance 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

Required Configuration for Exploitation

Possible impacted features are being evaluated at this time.

Indicators of Compromise

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.

Possible indicators of compromise are being evaluated at this time.

Mitigation

Possible mitigations are being evaluated at this time.

Resolution

This section will be updated once fixed releases are 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:

Subscribe to 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.