Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

Description

Many of Arista's products utilize industry-standard server hardware platforms. Periodically, vulnerabilities are identified within the underlying server components, which are documented and published by the OEM hardware vendor as security advisories. This advisory provides a consolidated reference of such vulnerabilities affecting the server hardware used by specific Arista SKUs.

Arista is not aware of any malicious exploitation of these vulnerabilities in customer networks. Customers are advised to verify their hardware configuration and apply the necessary mitigations.

Vulnerability Assessment

Affected Platforms

Arista SKUs in the following categories utilize Dell server hardware. Security vulnerabilities may exist in the underlying server components depending on the server model and configuration.

CloudVision Appliance (CVA)

The vulnerabilities detailed in the Resolved CVEs section can be mitigated by following the remediation procedures outlined in the Resolution section, which applies to customers utilizing the specified hardware SKUs.

- DCA-250-CV
- DCA-300-CV
- DCA-350E-CV

In the table, an X indicates the CVE can be resolved by following the steps detailed in the Resolution section.

CVEs Resolved by upgrading to CVA 7.2.0

CVE	DCA-250-CV
CVE-2024-38798	X
CVE	**DCA-300-CV, DCA-350E-CV**

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.

CVE-2024-38798	X
CVE-2024-42446	X
CVE-2025-11187	X
CVE-2025-15467	X
CVE-2025-15468	X
CVE-2025-15469	X
CVE-2025-31648	X
CVE-2025-66199	X
CVE-2025-68160	X
CVE-2025-69418	X
CVE-2025-69419	X
CVE-2025-69420	X
CVE-2025-69421	X
CVE-2026-22795	X
CVE-2026-22796	X

Danz Monitoring Fabric (DMF) Appliances

Server component updates for DMF appliances (DMF Controller, Analytics Node, Recorder Node, Service Node) are the responsibility of the customer. Customers should monitor the vendor's security advisory page filtering by the OEM product name that maps to the associated Arista SKU.

DMF SKU	OEM Product Name
DCA-DM-AA3, DCA-DM-CDL	PowerEdge R440
DCA-DM-AN450, DCA-DM-C450	PowerEdge R450
DCA-DM-RA3	PowerEdge R740XD
DCA-DM-RN760L, DCA-DM-SN760L, DCA-DM-RN760	PowerEdge R760XS
DCA-DM-SC2, DCA-DM-SC	PowerEdge R640
DCA-DM-SDL2, DCA-DM-SEL, DCA-DM-SDL	PowerEdge R740

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.

DCA-DM-SNR660	PowerEdge R660XS

Arista Guardian for Network Identity (AGNI) Appliance

Server component updates for AGNI appliances are the responsibility of the customer. Customers should monitor the vendor's security advisory page filtering by the OEM product name that maps to the associated Arista SKU.

AGNI SKU	OEM Product Name
DCA-AGNI-100	PowerEdge R450
DCA-AGNI-200	PowerEdge R470

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
  - 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
- Wi-Fi Access Points
- CloudVision CUE cloud service delivery
- CloudVision 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.

    - DCA-400-CV
    - DCA-450-CV
- CloudVision Portal on-premises, virtual appliance (including the CV-CUE on premises software)
- CloudVision Appliance Software
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- 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

No configuration exists.

Indicators of Compromise

Refer to the appropriate Dell advisory for specific Indicators of Compromise.

Mitigation

No mitigation exists.

Resolution

CloudVision Appliance (CVA)

1. **Option A**: Fresh Installation - Reimage the CVA appliance using the CVA 7.2.0 ISO. A fresh installation automatically updates BIOS and iDRAC firmware to the qualified versions bundled with CVA 7.2.0. Refer to the “Fresh Install of CVA 7” and "Initial Setup (First Boot) of CVA” sections of the CVA 7.2.0 TOI for installation and post-install setup procedures to redeploy the CVP and CVX workloads.
2. **Option B**: Upgrade the existing CVA to 7.2.0 using the standard upgrade path, then manually update BIOS and iDRAC to the recommended firmware versions detailed in the Recommended Firmware Versions section via the iDRAC management interface. Refer to the “Upgrade from CVA” section of the CVA 7.2.0 TOI for upgrade procedures. Obtain the specified firmware from Dell's website and proceed according to their provided upgrade guidelines.

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.

Recommended Firmware Versions

SKU	BIOS	iDRAC
DCA-250-CV	2.26.1	7.00.00.183
DCA-300-CV	1.20.2	7.30.10.50
DCA-350-CV	1.20.2	7.30.10.50

DANZ Monitoring Fabric (DMF) Appliances

DMF customers are advised to regularly check the vendor advisory page at https://www.dell.com/support/security/en-us for security updates and potential mitigations specific to their server configurations.

Arista Guardian for Network Identity (AGNI) Appliance

AGNI customers are advised to regularly check the vendor advisory page at https://www.dell.com/support/security/en-us for security updates and potential mitigations specific to their server configurations.

Hotfix

There are no hotfixes 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
- 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.