**Date:** October 22, 2025

| Revision | Date | Changes |
|---|---|---|
| 1.0 | October 22, 2025 | Initial release |

The following issues were discovered in Arista DANZ Monitoring Fabric (DMF). These issues affect DMF, Converged Cloud Fabric (CCF), CloudVision Appliance (CVA), and Multi-Cloud Director (MCD).

Issues covered in this Advisory:

1. CVE-2025-54545 Local privilege escalation from the CLI
2. CVE-2025-54546 SSH Port forwarding available to restricted users
3. CVE-2025-54547 In multiplexed ssh, sftp/scp operations possible after session timeout
4. CVE-2025-54548 Config database visible to restricted users through debug API
5. CVE-2025-54549 Update image verification bypass

## Description

**CVE-2025-54545**
**Description**: On affected platforms, a restricted user could break out of the CLI sandbox to the system shell and elevate their privileges.
CVSSv3.1 Base Score: 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Common Weakness Enumeration: CWE-732 (Incorrect Permission Assignment for Critical Resource)
This vulnerability is being tracked by BUG1084524 (CVA) / BSC-20739 (DMF, CCF, MCD)

**CVE-2025-54546**
**Description**: On affected platforms, restricted users could use SSH port forwarding to access host-internal services
CVSS:3.1 Base Score 7.5 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
Common Weakness Enumeration: CWE-732 (Incorrect Permission Assignment for Critical Resource)
This vulnerability is being tracked by BUG1084523 (CVA) / BSC-20747 (DMF, CCF, MCD)

**CVE-2025-54547**
**Description**: On affected platforms, if SSH session multiplexing was configured on the client side, SSH sessions (e.g, scp, sftp) multiplexed onto the same channel could perform file-system operations after a configured session timeout expired
CVSS:3.1 Base Score 5.3 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L)
Common Weakness Enumeration: CWE-613 (Insufficient Session Expiration)
This vulnerability is being tracked by BUG1084527 (CVA) / BSC-20748 (DMF, CCF, MCD)

**CVE-2025-54548**

**Description**: On affected platforms, restricted users could view sensitive portions of the config database via a debug API (e.g., user password hashes)
CVSS:3.1 Base Score 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)
Common Weakness Enumeration: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)
This vulnerability is being tracked by BUG1082430 (CVA) / BSC-20741 (DMF, CCF, MCD)

**CVE-2025-54549**
**Description**: Cryptographic validation of upgrade images could be circumventing by dropping a specifically crafted file into the upgrade ISO
CVSS:3.1 Base Score 5.9 (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:N)
Common Weakness Enumeration: CWE-347 (Improper Verification of Cryptographic Signature)
This vulnerability is being tracked by BUG1121566 (CVA) / BSC-20815 (DMF, CCF, MCD)

These issues were discovered during Arista sponsored penetration testing and Arista is not aware of any malicious uses of this issue in customer networks.

## Vulnerability Assessment

### Affected Software

#### Danz Monitoring Fabric

- DMF 8.7.0
- DMF 8.6.1 and below releases on the DMF 8.6.x release train
- DMF 8.5.2 and below releases on the DMF 8.5.x release train
- DMF 8.4.5 and all below versions

#### Converged Cloud Fabric

- CCF 6.2.4 and all below versions

#### CloudVision Appliance software

- All versions of CVA 7.0.x

#### Multi-Cloud Director

- MCD 2.4.0 and all below versions

## Affected Platforms

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

- CloudVision DCA Appliances running CloudVision Appliance 7.0.x software:
    - DCA-350E-CV
    - DCA-300-CV
    - DCA-250-CV
    - DCA-200-CV

  Note: CloudVision Portal virtual appliance software is not affected.

- Arista Converged Cloud Fabric (formerly Big Switch BCF)
    - all physical and virtual appliances
- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)
    - all physical and virtual appliances
- Arista Multi-Cloud Director
    - all virtual appliances

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
    - 7010 Series
    - 7010X Series
    - 7020R Series
    - 7130 Series running EOS
    - 7150 Series
    - 7160 Series
    - 7170 Series
    - 7050X/X2/X3/X4 Series
    - 7060X/X2/X4/X5/X6 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3/R4 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/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 Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal, virtual appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista 7130 Systems running MOS
- 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

1. CVE-2025-54545: The following conditions must be met: A non-administrator user must be able to log into on the system, either via a local-user configuration or via remote authentication (TACACS+/RADIUS).
2. CVE-2025-54546: The following conditions must be met: A non-administrator user must be able to log into on the system, either via a local-user configuration or via remote authentication (TACACS+/RADIUS); the non-administrator user must have CLI access.
3. CVE-2025-54547: The following conditions must be met: The connecting SSH client must be configured to allow multiple sessions to be multiplexed onto the same SSH Connection (e.g., via the OpenSSH **ControlMaster auto** configuration or other equivalent configurations); The ControlMaster connection must be active; The attacker must have access to the ControlMaster socket on the client.
4. CVE-2025-54548: The following conditions must be met: A non-administrator user must be configured on the system; The user must have REST API access.
5. CVE-2025-54549: The operator must attempt to install a tampered software upgrade image.

## Indicators of Compromise

1. CVE-2025-54545: A configured external audit log would show the use of **debug developer** by a non-admin user

   The audit record will contain **AUDIT EVENT: CLI_COMMAND, cmd-args="debug developer"** and **user="<some-non-admin-user>"**.

```
2025-09-09T06:46:20.533Z floodlight: INFO  LOCLAUD1001: AUDIT EVENT: CLI_COMMA
ND auth-description="session/da67822855f50c23da34f3c7adfa1338cb75b4aa2c9c2159b
```

```
aa70c27e0277b29" user="ro" remote-address="10.95.66.26" session-id="da67822855
f50c23da34f3c7adfa1338cb75b4aa2c9c2159baa70c27e0277b29" cmd-args="debug develo
per " duration-ms="3.772" start-time="2025-09-09T06:46:20.524361Z"
```

An example of the indicators of compromise for CVE-2025-54545

2. CVE-2025-54546: No indicators of compromise exist
3. CVE-2025-54547: No indicators of compromise exist
4. CVE-2025-54548: No indicators of compromise exist
5. CVE-2025-54549: A downloaded upgrade image can be manually checked against the hash values published on arista.com. If the published hash values do not match those of the image this is a potential indicator of compromise.

## Mitigation

1. CVE-2025-54545: Disable any non-administrator users until an upgraded version can be installed.
2. CVE-2025-54546: Disable any restricted users until an upgraded version can be installed.
3. CVE-2025-54547: No known mitigation
4. CVE-2025-54548: Disable any restricted users until an upgraded version can be installed.
5. CVE-2025-54549: A downloaded upgrade image can be manually checked against the hash values published on arista.com.
   If the published hash values do not match those of the image this is a potential indicator of compromise.

## 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. Fixed versions are as follows for each product:

### Danz Monitoring Fabric

- DMF 8.7.1 and later releases in the 8.7.x train
- DMF 8.6.2 and later releases in the 8.6.x train
- DMF 8.5.3 and later releases in the 8.5.x train
- DMF 8.4.6 and later releases in the 8.4.x train.

### Converged Cloud Fabric

- CCF 6.2.5 and later releases in the 6.2.x train

**Cloud Vision Appliance**

- CVA 7.1.0 and later releases in the CVA 7.x train

**Multi-Cloud Director**

- MCD 2.4.1 and later releases in the 2.4.x train

## 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