Date: November 18, 2025

Revision	Date	Changes
1.0	November 18, 2025	Initial release

The following issues were discovered during regular penetration testing of Arista's EOS. Issues detailed cover CloudVision Exchange (CVX) based features including Media Control Services (MCS).

Issues covered in this Advisory:

1. CVE-2025-5088 - An authenticated Redis session could be used to obtain full root access to all servers in the CVX cluster
2. CVE-2025-5089 - Malformed messages received from the connected CVX server can cause SysDB agent crashes.
3. CVE-2025-5090 - Unexpected messages from a connected switch may lead to agent crashes on CVX causing instability in the CVX cluster.

Description

MCS Redis Issue (CVE-2025-5088)

Description: With CVE-2025-5088, an authenticated Redis session could be used to obtain full root access to all servers in the CVX cluster. Note that this would require an attacker to have both network access to the Redis service on a CVX server and the Redis password. Please note that all Redis communication, including authentication, occurs over plaintext in the present day. TLS support is tracked under RFE1294850.
CVSSv3.1 Base Score: 8.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L)
CVSSv4.0 Base Score: 8.7 (AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-269: Improper Privilege Management
This vulnerability is being tracked by BUG1140117

Sysdb Crashes (CVE-2025-5089)

Description: In a CVX cluster, an EOS switch connected to a CVX server is not resilient to certain malformed messages received from the connected CVX server. Similarly, the CVX server is not resilient to certain malformed messages received from the connected EOS switch. This leads to either a Sysdb agent crash on the EOS device causing a soft reset of the switch or agent crashes on the CVX server causing instability of the CVX cluster. An attacker could use this behavior to create a denial of service (DoS) scenario. Note that this would require the attacker to already have a high privilege access to the connected device to be able to send custom TCP packets. EOS switches that are not connected to a CVX server are not impacted.
CVSSv3.1 Base Score: 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 7.1 (AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N)

Common Weakness Enumeration: CWE-20: Improper Input Validation
This vulnerability is being tracked by BUG1140255

Switch disconnects (CVE-2025-5090)

Description:CVX is not resilient to unexpected messages from a connected switch. This leads to agent crashes on CVX causing instability in the CVX cluster. An attacker could use this behavior to create a denial of service (DoS) scenario. Note that this would require the attacker to have a high privilege access to the connected switch to be able to send custom TCP packets to the CVX.
CVSSv3.1 Base Score: 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 7.1 (AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-20: Improper Input Validation
This vulnerability is being tracked by BUG1139764

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

EOS Versions

CVE-2025-5088 and CVE-2025-5089

- 4.34.1F and below releases in the 4.34.x train
- 4.33.4M and below releases in the 4.33.x train
- 4.32.6M and below releases in the 4.32.x train
- 4.31.8M and below releases in the 4.31.x train
- All releases in the 4.30.x train

CVE-2025-5090

- 4.34.1F and below releases in the 4.34.x train
- 4.33.4M and below releases in the 4.33.x train
- 4.32.6M and below releases in the 4.32.x train
- All releases in the 4.31.x train
- All releases in the 4.30.x train

Affected Platforms

CVE-2025-5088 and CVE-2025-5090

The following products **are** affected by these vulnerabilities:

- Arista EOS-based products:
    - CloudVision eXchange, virtual or physical appliance

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

- Arista EOS-based products:
    - 710/710X 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
- 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)
- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

CVE-2025-5089

The following products **are** affected by these vulnerabilities:

- Arista EOS-based products:
  - CloudVision eXchange, virtual or physical appliance

- Arista EOS-based products (affected only when connecting to affected CloudVision eXchange product):
  - 710/710X 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

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)
- 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

In order to be vulnerable to CVE-2025-5088, the following condition must be met:

MCS Service must be configured:

```
cvx1#show cvx service mcs
Mcs
  Status: Enabled
  Supported versions: 1

  Switch    Status    Negotiated Version
  ------    -------   ------------------
  <Switch1> Enabled   1

cvx1#show running-config section mcs
cvx
   service mcs
      redis password 7 03054902151B20
      no shutdown
```

If MCS Service is not configured there is no exposure to this issue and the message will look like:

```
cvx1#show cvx service mcs
Mcs
  Status: Disabled
  Supported versions: 1

  Switch    Status     Negotiated Version
  ------    --------   ------------------
  <Switch1> Disabled
```

In order to be vulnerable to CVE-2025-5089 and CVE-2025-5090, the following condition must be met:

CVX must be configured:

```
cvx1#show cvx
  Status: Enabled
  Mode: Standalone
  Heartbeat interval: 20.0
  Heartbeat timeout: 60.0
  Client connection state preserving: Disabled

cvx1#show running-config section cvx
cvx
   no shutdown
```

Indicators of Compromise

MCS Redis Issue (CVE-2025-5088)

There is no indicator of compromise for this issue

Sysdb Crashes (CVE-2025-5089)

There is no indicator of compromise for this issue

Switch disconnects (CVE-2025-5090)

When CVE-2025-5090 is hit, the ControllerOob agent will disconnect one of the clients regularly and syslogs of the the following pattern can be observed:

```
Aug 12 02:45:07 CVX-A1 ControllerOob: %CVX-6-CLIENT_DEREGISTRATION: CVX client 2c-dd-
```

```
e9-4e-6c-ab (10.90.11.3) has deregistered.
Aug 12 02:45:07 CVX-A1 Controllerdb: %FWK-3-SOCKET_CLOSE_LOCAL: Closing connection to
 Sysdb (pid:3222) at tbt://10.90.11.3:9999<10.90.11.51:>/ (ConnectionManager disconne
ct)
Aug 12 02:45:07 CVX-A1 Controllerdb: %FWK-3-MOUNT_PEER_CLOSED: Peer closed socket con
nection. (tbt://10.90.11.3:9999<10.90.11.51:>/-in)(Sysdb (pid:3222))
```

Mitigation

MCS Redis Issue (CVE-2025-5088)

To run the redis-server as a dedicated "redis" user and group on the CVX server, follow these steps, ensuring all changes are applied correctly and the service restarts smoothly. This approach enhances security by isolating the Redis process with its own user and group permissions.

Please ensure that these mitigation steps are tested thoroughly in a non-production environment prior to production deployment.

1. **Log in to the CVX Server**
   Access your CVX server (e.g. using SSH) using the appropriate credentials. This is the initial point of access for all subsequent configuration changes.
2. **Stop Redis Before Applying Changes**
   It is crucial to stop Redis to prevent data corruption or conflicts while modifying its configuration.
   This is achieved by unconfiguring the Redis password on the MCS service.

   Executing **no redis password** stops the Redis service by removing its authentication credentials, which prevents it from running.

```
cvx>enable
cvx#config
cvx(config)#cvx
cvx(config-cvx)#service mcs
cvx(config-cvx-mcs)#no redis password
cvx(config-cvx-mcs)#
```

3. **Edit the *redis.service* Systemd Service File**
   This step involves modifying the systemd service file for Redis to specify the dedicated user and group under which Redis will run.

   First, transition to bash mode from the CVX configuration prompt:

```
cvx(config-cvx-mcs)#bash
```

Once in bash, use ***sudo nano*** to edit the ***redis.service*** file:

```
[cvx ~]$sudo nano /etc/systemd/system/redis.service
```

4. **Add 'User' and 'Group' Directives to the *[Service]* Section**
   Within the **redis.service** file, locate the **[Service]** section and add the following lines:

```
[Service]
User=redis
Group=redis
```

   This modification ensures that when the **redis-server starts**, it will execute under the context of the **redis** user and **redis** group, thereby enforcing stricter access controls and enhancing system security.

   Save and exit the editor.

5. **Change Ownership of the Redis Log File**
   To ensure the **redis** user has appropriate write permissions for its log file, change the ownership of **/var/log/redis/redis.log** to the **redis** user and group.

```
[cvx ~]$sudo chown redis:redis /var/log/redis/redis.log
```

   This step is required for the Redis server to be able to write logs once it restarts under the new user and group.
6. **Restart the Redis with New Changes**
   After making all necessary modifications, restart the Redis to apply the new configuration. This is done by reconfiguring the Redis password, which will bring the service back online.

   First, exit bash mode:

```
[cvx ~]$exit
```

   Then, reconfigure the Redis password:

```
cvx(config-cvx-mcs)#redis password <secret>
```

Replace **<secret>** with your actual Redis password. This action will re-enable the Redis, and it will now run with the specified **redis** user and **redis** group.

NOTE: Following a CVX server reload or power cycle, all previously mentioned steps must be repeated.

Sysdb Crashes (CVE-2025-5089)

There is no mitigation for this issue

Switch disconnects (CVE-2025-5090)

There is no mitigation for this issue

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-2025-5088 and CVE-2025-5089 have been fixed in the following releases:

- 4.34.2F and later releases in the 4.34.x train
- 4.33.5M and later releases in the 4.33.x train
- 4.32.7M and later releases in the 4.32.x train
- 4.31.9M and later releases in the 4.31.x train

CVE-2025-5090 has been fixed in the following releases:

- 4.34.2F and later releases in the 4.34.x train
- 4.33.5M and later releases in the 4.33.x train
- 4.32.7M and later releases in the 4.32.x train

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 security

notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:>/p>

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