Date: May 19, 2026

Revision	Date	Changes
1.0	May 19, 2026	Initial release

The CVE-ID tracking this issue: CVE-2025-49844
CVSSv3.1 Base Score: 9.9 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
CVSSv4.0 Base Score: 9.4
(CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-416 Use After Free
This vulnerability is being tracked by BUG1140119 and BUG1391625

Description

On affected Arista platforms running Media Control Service (MCS) on CloudVision eXchange (CVX) or DANZ Monitoring Fabric (DMF), an authenticated user—one who has already gained access to the system—may be able to trigger a memory corruption condition that can potentially lead to remote code execution.

Note: DMF in its default condition is not affected. The vulnerability is only present in DMF under unusual, user enabled configurations.

Arista has not received reports of malicious exploitation at this time.

Vulnerability Assessment

Affected Software

EOS Versions

Only Media Control Service (MCS) on CloudVision eXchange (CVX) is affected with the following versions:

- 4.34.1F and below releases in the 4.34.x train
- 4.33.7M and below releases in the 4.33.x train
- 4.32.10M and below releases in the 4.32.x train
- All releases in trains older than 4.32.x

DMF Versions

- DMF 8.7.2 and below releases in the 8.7.x train
- DMF 8.8.0

Affected Platforms

Media Control Service (MCS)

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

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

Arista DANZ Monitoring Fabric (DMF)

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

- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)

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
- 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 - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- 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-2025-49844, the following condition must be met:

Media Control Service (MCS)

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-2025-49844, 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
```

Arista DANZ Monitoring Fabric (DMF)

Network ACL is misconfigured to allow more than DMF Controller IPs:

```
an1> show cluster access-control access-list redis
an1(config-cluster-access-list)# show cluster access-control access-list redis
# Access-list Rule Action Source
-|-----------|----|------|-----------|
1 redis       1    permit 0.0.0.0/0
an1(config-cluster-access-list)# show cluster access-control access-list replicated-
redis
# Access-list Rule Action Source
-|-----------|----|------|-----------|
1 replicated-redis       1    permit 0.0.0.0/0
```

With the default configuration and when DMF controller(s) (e.g 10.2.3.4) is allowed to connect

there is no exposure to this issue. The CLI config's looks like:

```
an1> show cluster access-control access-list redis
None.
an1> show cluster access-control access-list replicated-redis
None.

an1(config-cluster-access-list)# show cluster access-control access-list redis
# Access-list Rule Action Source
-|-----------|----|------|-----------|
1 redis       1    permit 10.2.3.4/32
an1(config-cluster-access-list)# show cluster access-control access-list replicated-
redis
# Access-list Rule Action Source
-|-----------|----|------|-----------|
1 replicated-redis       1    permit 10.2.3.4/32
```

Indicators of Compromise

Media Control Service (MCS)

There is no indicator of compromise for this issue

Arista DANZ Monitoring Fabric (DMF)

Confirm that only DMF controller IPs (10.2.3.4) are seen with command:

```
sudo tcpdump -i any '(port 6379 or port 9379)' -n -l | grep -E 'bond0|bond3' | grep -
E 'In  IP'

19:00:26.234556 bond0 In  IP 10.2.3.4:55696 > 10.240.145.2.redis: Flags [P.], seq 368
04:36818, ack 299, win 502, options [nop,nop,TS val 996795373 ecr 751259688], length
14: RESP "PING"

19:00:26.234836 bond0 In  IP 10.2.3.4.55696 > 10.240.145.2.redis: Flags [.], ack 306,
 win 502, options [nop,nop,TS val 996795373 ecr 751269689], length 0

19:00:26.234958 bond0 In  IP 10.2.3.4.33670 > 10.240.145.2.9379: Flags [P.], seq 477:
491, ack 79, win 502, options [nop,nop,TS val 996795373 ecr 751259689], length 14
```

The following log audit may reveal an instance of a successful attack

```
sudo grep -Ei "lparser\.c|lbaselib\.c|SIGSEGV|RediShell" /var/log/analytics/

=== REDIS BUG REPORT START: Cut & paste starting from here === 1234:M 03 Oct 2025 14:
20:10.555 # Redis 7.4.5 crashed by signal: 11 (SIGSEGV) 1234:M 03 Oct 2025 14:20:10.5
55 # Failed assertion: <no assertion failed> 1234:M 03 Oct 2025 14:20:10.555 # --- ST
ACK TRACE --- /usr/local/bin/redis-server 0x12345678 (logStackTrace+0x4d) /lib/x86_64
-linux-gnu/libc.so.6+0x42520 /usr/local/bin/redis-server 0x456789ab (luaY_parser+0x18
3) at deps/lua/src/lparser.c:387 /usr/local/bin/redis-server 0x89abcdef (luaD_precall
+0x242) at deps/lua/src/ldo.c:312 /usr/local/bin/redis-server 0x01234567 (lua_eval+0x
110) at src/scripting.c:750 /usr/local/bin/redis-server 0xabcdef01 (evalGenericComman
d+0x205) at src/scripting.c:1020 /usr/local/bin/redis-server 0x23456789 (call+0xc4) a
t src/server.c:3950 /usr/local/bin/redis-server 0x3456789a (processCommand+0x5d2) at
src/server.c:4510 === REDIS BUG REPORT END ===
```

Mitigation

Media Control Service (MCS)

Follow these organized steps to implement an event handler on CVX that restricts access to sensitive Redis commands.

Step 1: Authenticate to the CVX Server

Login to the CVX server with administrative credentials to start the configuration.

Step 2: Generate the Restriction Script

Develop the script **restrict-redis-commands.sh** by incorporating the necessary logic to block the execution of specific commands as detailed below:

```
#!/bin/bash
# Denied commands:
# eval, evalsha, config, acl, script, debug, shutdown

REDIS_PASS=$(sudo grep -m1 '^requirepass' /etc/redis/redis.conf | awk '')
AUTH_ARGS=""
if [ -n "$REDIS_PASS" ]; then
   AUTH_ARGS="-a $REDIS_PASS"
fi

USERS=$(redis-cli $AUTH_ARGS ACL LIST | sed -n 's/^user \([^ ]*\).*/\1/p')
for user in $USERS; do
   redis-cli $AUTH_ARGS ACL SETUSER "$user" \
     -eval \
     -evalsha \
```

```
    -script \
    -config \
    -acl \
    -debug \
    -shutdown
done
```

Step 3: Transfer the Script to the CVX Server

Place the file within the **/mnt/flash/** directory on your CVX server using one of the following methods:

- **Option A: Remote Transfer** — Utilize the **copy** command to pull the script from a remote host. For instance, using SCP:

```
cvx#copy scp:<user@host>:<path_to_script> flash:
```

- **Option B: Local Creation** — Use the CVX bash shell to create the file and paste the script contents directly:

```
cvx#bash
[user@cvx ~]$ nano /mnt/flash/restrict-redis-commands.sh
```

Step 4: Establish the Event Handler

Access the CLI configuration mode to run the series of commands provided below. In this instance, the event-handler is identified by the name **restrict-redis-commands**.

```
event-handler restrict-redis-commands
   action bash /mnt/flash/restrict-redis-commands.sh
   delay 0
   trigger on-logging
      regex Started Redis
```

Step 5: Confirm and Persist Changes

Verify the event handler status:

```
cvx#show event-handler restrict-redis-commands
```

Once confirmed, save the running configuration to memory:

```
cvx#write
```

IMPORTANT: For High Availability (HA) deployments, these steps must be performed on every CVX server in the cluster.

CAUTION: Implementing these command restrictions may affect custom scripts or third-party integrations that interact with Redis. Test in a non-production environment first.

Arista DANZ Monitoring Fabric (DMF)

Correctly configure network ACLs for DMF controller IP(s). Example 10.2.3.4.

```
an1(config-cluster-access-list)# show cluster access-control access-list redis
# Access-list Rule Action Source
-|-----------|----|------|-----------|
1 redis       1    permit 10.2.3.4/32
an1(config-cluster-access-list)# show cluster access-control access-list replicated-
redis
# Access-list Rule Action Source
-|-----------|----|------|-----------|
1 replicated-redis       1    permit 10.2.3.4/32
```

Resolution

Media Control Service (MCS)

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-2025-49844 has been fixed in the following releases:

- 4.32.11 and later releases in the 4.32.x train
- 4.33.8 and later releases in the 4.33.x train
- 4.34.2 and later releases in the 4.34.x train

Arista DANZ Monitoring Fabric (DMF)

If the network ACLs are correctly configured as shown in Mitigation, the risk is mitigated. However, Arista recommends upgrading to a remediated version when available for defense-in-

depth.

CVE-2025-49844 has been fixed in the following releases:

- DMF 8.7.3 and later release in the 8.7.x train
- DMF 8.8.1 and later release in the 8.8.x train
- DMF 8.9.0 and later release in the 8.9.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:

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