**Date: February 20, 2024**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | February 20, 2024 | Initial release |

The CVE-ID tracking this issue: CVE-2023-6068
CVSSv3.1 Base Score: 3.1 (AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N)
Common Weakness Enumeration: CWE-283 Improper Access Control
This vulnerability is being tracked by BUG 869667

# Description

On affected 7130 Series FPGA platforms running MOS and recent versions of the MultiAccess FPGA, application of ACL's may result in incorrect operation of the configured ACL for a port resulting in some packets that should be denied being permitted and some packets that should be permitted being denied.

This issue was discovered internally and Arista is not aware of any malicious uses of this issue in customer networks.

# Vulnerability Assessment

## Affected Software

- MultiAccess FPGA Software version 1.7.1 (when running with MOS)
- MultiAccess FPGA Software version 1.6.x (when running with MOS)

## Affected Platforms

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

- Arista MOS-based products:
    - 7130 Series FPGA running MultiAccess version 1.7.1 or 1.6.x

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

    - 7130 Series running EOS
    - 7020R Series
    - 7150 Series
    - 7160 Series
    - 7170 Series
    - 7050X/X2/X3/X4 Series
    - 7060X/X2/X4/X5 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2/R3 Series
    - 7800R3 Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - AWE 5000 Series
- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and 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)

## Required Configuration for Exploitation

In order to be vulnerable to CVE-2023-6068, the following condition must be met:

MOS must be configured with MultiAccess FPGA software versions 1.7.1 or 1.6.x and can be determined by running the show version command and referring to the highlighted section as shown below.

```
switch(config)#show version
Device: Metamako MetaMux 48 with L-Series
SKU: DCS-7130-48LB
```

```
Serial number: M48LB-A3-27719-4

Software image version: 0.39.0alpha4
Internal build ID: master+9345
Applications: multiaccess-1.7.1
```

As shown above this switch is running a vulnerable version of the MultiAccess program, v1.7.1.

## Indicators of Compromise

This vulnerability may lead to forwarding of packets that should be blocked by an ACL on a port.

Once triggered, the ACL filter on a port applies ACL decisions from the previous packet to the current packet and remains stuck in this state until the FPGA is reloaded. This is not detectable at the command line and is not visible in any counter state recorded by the device.

## Mitigation

The workaround is to only apply one access-list to any particular port after the MultiAccess image is loaded into the FPGA. If a new access-list is to be applied to a port, the FPGA image should be reloaded after the access-list is applied.

Run the following commands to reload the FPGA image, where the line in yellow represents new access control lists to be added:

```
switch(config-app-multiaccess)#shut
switch(config-app-multiaccess)#multiaccess-group 0 client 0 access-
list new_acl_if_need
switch(config-app-multiaccess)#no shut
```

The previous applied access control lists will automatically apply after FPGA reload.

## 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.

CVE-2023-6068 has been fixed in the following releases:

- MultiAccess FPGA 1.8.0 and later

## Hotfix

There is no available hotfix

## 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: 408-547-5502 ; 866-476-0000
Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support