Date: June 25, 2024

Revision	Date	Changes
1.0	June 25, 2024	Initial release

The CVE-ID tracking this issue: CVE-2024-4578
CVSSv3.1 Base Score: 8.4 (CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)
Common Weakness Enumeration: CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

This vulnerability is being tracked by BUG948397

Description

This Advisory describes an issue that impacts Arista Wireless Access Points. Any entity with the ability to authenticate via SSH to an affected AP as the “config” user is able to cause a privilege escalation via spawning a bash shell. The SSH CLI session does not require high permissions to exploit this vulnerability, but the config password is required to establish the session. The spawned shell is able to obtain root privileges.

This issue was reported by an external source. Arista is not aware of any malicious uses of this issue in customer networks.

Arista would like to acknowledge and thank David Miller from cyllective AG (https://cyllective.com) for responsibly reporting CVE-2024-4578.

Vulnerability Assessment

Affected Software

Wi-Fi Access Point Software:

- 13.0.2-28-vv1002 and earlier releases in the 13.0.2.x train
- All releases in the 15.x train
- 16.1.051-vv6 and earlier versions are affected in the 16.x train.

Affected Platforms

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

- All Arista Wifi Access Points

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 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
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista 7130 Systems running MOS
- 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)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2024-4578, the following condition must be met:

The user must have knowledge of the config shell password to gain initial access.

Indicators of Compromise

A list of all commands executed is saved in /var/log/cli.log file. The logs can be viewed by generating a debug bundle and viewing the var/log/cli.log file within the generated debug bundle.

```
cat /var/log/cli.log
2024.06.08 00:09:38.052413 INFO cli (cli.-.load_commands_from_yaml) (9494:9494): Took
 31770831 ns to load commands
```

An example of this issue being exploited is not included above since that could reveal excessive information. Admins reviewing /var/log/cli.log should look for instances of bash shell code commands being run as a part of CLI commands.

Mitigation

To mitigate the attack, configure a strong config shell password and share the password only with admin and/or trusted parties.

Resolution

Arista recommends customers move to the latest version of each release that contains all the fixes listed below:

CVE-2024-4578 has been fixed in the 13.x and 16.x release trains, as follows:

- 13.0.2-28-vv1101 and later releases in the 13.0.2.x train
- 16.1.0-51-vv703 and later releases in the 16.1.0.x train

For more information about upgrading WiFi AP Software, please see Upgrade Server and Upgrading Firmware of Wi-Fi Access Points with On-Premises Wireless Manager

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