

Date: April 11, 2023

Revision	Date	Changes
1.0	April 11, 2023	Initial release

This advisory consists of two CVEs which affect the Arista CloudEOS product.

CVE-ID: CVE-2023-24545

CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Common Weakness Enumeration: CWE-400- Uncontrolled Resource Consumption

This vulnerability is being tracked by BUG 743423

CVE-ID: CVE-2023-24513

CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L)

Common Weakness Enumeration: CWE-126 - Buffer Over-read

This vulnerability is being tracked by BUG 764777

Description

This advisory details the impact of two issues discovered on Arista CloudEOS;

CVE-2023-24545: On affected platforms running Arista CloudEOS an issue in the Software Forwarding Engine (Sfe) can lead to a potential denial of service attack by sending malformed packets to the switch. This causes a leak of packet buffers and if enough malformed packets are received, the switch may eventually stop forwarding traffic.

CVE-2023-24513: On affected platforms running Arista CloudEOS a size check bypass issue in the Software Forwarding Engine (Sfe) may allow buffer over reads in later code. Additionally, depending on configured options this may cause a recomputation of the TCP checksum which could be leveraged in DDoS attacks.

These issues were discovered internally and Arista is not aware of any malicious uses of these issues in customer networks.

Vulnerability Assessment

Affected Software

CVE-2023-24545

CloudEOS Versions

- 4.29.1F and below releases in the 4.29.x train
- 4.28.4M and below releases in the 4.28.x train
- 4.27.7M and below releases in the 4.27.x train
- 4.26.8M and below releases in the 4.26.x train

CVE-2023-24513

CloudEOS Versions

- 4.29.1F and below releases in the 4.29.x train
- 4.28.5M and below releases in the 4.28.x train
- 4.27.8M and below releases in the 4.27.x train
- 4.26.9M and below releases in the 4.26.x train

Affected Platforms

CVE-2023-24545 and CVE-2023-24513

The following products are affected by CVE-2023-24545 and CVE-2023-24513:

- All CloudEOS software forwarding instances, including:
 - All supported hypervisor deployments
 - DCA-200-VEOS appliances
 - AWS Marketplace
 - Azure Marketplace
 - Google Cloud Platform marketplace
 - Equinix Network Edge

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

- Arista EOS-based Hardware products:
 - 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 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
- cEOS-lab
- vEOS-lab
- 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
- 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 - Formerly Untangle (Formerly Arista NG Firewall and Arista Micro Edge)
- Arista Unified Cloud Fabrics - (Formerly Pluribus Netvisor One)

Required Configuration for Exploitation

CVE-2023-24545 and CVE-2023-24513

In order to be vulnerable to CVE-2023-24545 and CVE-2023-24513, the switch must be configured to run the Software Forwarding Engine (Sfe). Sfe is the default configuration on CloudEOS platforms.

```
switch(config)#show agent Sfe uptime
Agent Name      Restarts      Uptime
-----
Sfe              1             0:29:49
```

Indicators of Compromise

CVE-2023-24545

The following two indicators in combination might indicate system compromise for CVE-2023-24545:

#1 - The Sfe agent log will print warning messages once the number of packet buffers is reaching low levels (< 25% Buffers free). The command `show agent Sfe logs` will include lines such as below:

```
I0719 13:58:07.  
860103 2994 Management.cpp:681] Possible Packet Leak: <25% Buffers free(1273/131072)
```

#2 - Additionally, the command `show platform sfe counters | nz | grep -i frag` can be used to see if the platform is receiving fragmented packets. In particular, look for large values in the counter:

```
ForUsClassifyIpv4-frag_recv_pkts          ForUsClassifyIpv4          module          packet  
s 353771
```

CVE-2023-24513

No indications of compromise exists.

Mitigation

CVE-2023-24545 and CVE-2023-24513

There is no mitigation / workaround for these issues.

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-2023-24545

CVE-2023-24545 has been fixed in the following releases:

- 4.29.2F and later releases in the 4.29.x train
- 4.28.5M and later releases in the 4.28.x train
- 4.27.8M and later releases in the 4.27.x train
- 4.26.9M and later releases in the 4.26.x train

CVE-2023-24513

CVE-2023-24513 has been fixed in the following releases:

- 4.29.2F and later releases in the 4.29.x train
- 4.28.6M and later releases in the 4.28.x train
- 4.27.9M and later releases in the 4.27.x train

- 4.26.10M and later releases in the 4.26.x train

Hotfix

The following hotfixes can be applied to remediate both CVE-2023-24545 and CVE-2023-24513. Due to the size of the hotfixes, there are multiple files. Each hotfix applies to a specific set of release trains:

Note: Installing/uninstalling the SWIX will cause Sfe agent to restart and stop forwarding traffic for up to 10 seconds.

4.29.1F and below releases in the 4.29.x Train:

URL: [SecurityAdvisory85_4.29_Hotfix.swix](#)

SWIX Hash:

SHA512

```
(SHA-512)c965e149cbbaa8698648af9290c5a728e9fe635186eee7629b789502ef37db4a94beea5ecd20e1dc8a19c2cc8988052b625cfccf764c28b8b0e9e4eef8e79bb4
```

4.28.5M and below releases in the 4.28.x train:

URL: [SecurityAdvisory85_4.28_Hotfix.swix](#)

SWIX Hash:

```
(SHA-512)522d51c6548111d9819ef8b1523b8798ac6847012955e3f885c6f466c81468960fbd4497b45289c8f77297263111340fbdbd7003a30b64e3ef9a270ace62c079
```

4.27.8M and below releases in the 4.27.x train:

URL: [SecurityAdvisory85_4.27_Hotfix.swix](#)

SWIX Hash:

```
(SHA-512)5ce5479c11abf185f50d484204555b2dfb9b1c93e8f475d027082ca0951cbfca0f331960a1dd111b8c079264b1dab31b0a62c8daf011afb27b1283c2382747a2
```

4.26.9M and below releases in the 4.26.x train:

URL: [SecurityAdvisory85_4.26_Hotfix.swix](#)

SWIX Hash:

```
(SHA-512)9386f12a24f35679bdeb08d506bf0bddb9703d1ef3043de2c06d09ff47f2dd0d1bd7aca0748febb5b04fbdeaed7c4ae2922086fb638c754c3a9a5384306396d2
```

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>

