Date: April 5, 2024

Revision	Date	Changes
1.0	April 3, 2024	Initial release
1.1	April 5, 2024	Update required configuration for exploitation and mitigation

Description

Arista Networks is providing this security update in response to the following publicly disclosed security vulnerabilities related to HTTP/2 CONTINUATION frames. This set of vulnerabilities is the result of some HTTP/2 implementations that do not properly limit or sanitize the amount of CONTINUATION frames sent in a single stream. An attacker that can send packets to a target server can send a stream of CONTINUATION frames, which can result in an out-of-memory crash, enabling an attacker to launch a denial of service (DoS) attack against a target service using a vulnerable implementation.

The following CVEs are tracked as part of this announcement:

- CVE-2023-45288 tracks the Go packages net/http and net/http2 packages do not limit the number of CONTINUATION frames read for an HTTP/2 request.
- CVE-2024-28182 tracks the nghttp2 library will continue to receive CONTINUATION frames and will not callback to the application to allow visibility into this information before it resets the stream.
- CVE-2024-27316 tracks the Apache Httpd implementation does not properly append header information in memory, causing an OOM crash.
- CVE-2024-31309 tracks the Apache Traffic Server consuming more resources on the server in HTTP/2 CONTINUATION DoS attack.
- CVE-2024-27919 tracks the Envoy's HTTP/2 codec does not reset a request when header map limits have been exceeded.
- CVE-2024-30255 tracks the HTTP/2 protocol stack in Envoy versions 1.29.2 or earlier are vulnerable to CPU exhaustion due to flood of CONTINUATION frames. This allows an attacker to send a sequence of CONTINUATION frames without the END_HEADERS bit set causing CPU utilization, consuming approximately 1 core per 300Mbit/s of traffic.
- CVE-2024-2653 tracks the AMPHP implementation of HTTP/2 which will collect CONTINUATION frames in an unbounded buffer and will not check a limit until it has received the set END_HEADERS flag
- CVE-2024-2758 tracks the Tempesta FW rate limits are not enabled by default
- CVE-2024-27983 tracks the Node.js HTTP/2 server unavailable by sending a small amount of HTTP/2 frames packets with a few HTTP/2 frames inside

EOS running the affected releases are vulnerable to CVE-2023-45288 if any of the following features (The “EOS affected features list”) are enabled. Please see required configuration for exploitation to see what configuration needs to be in place to be vulnerable:

- TerminAttr: Used for streaming telemetry to Arista CloudVision.
- OpenConfig: Used for the OpenConfig standard which allows for both streaming telemetry and configuration.
- gRIBI: Used to insert entries in the routing table from an external client.
- Octa: Combines gNMI service support for OpenConfig and certain TerminAttr functionality.

Wifi Products must be using Openconfig based AP management to be vulnerable to CVE-2023-45288.

Note: the affected products do use golang grpc-go library with version vulnerable to CVE-2023-45288. But based on Arista's analysis of the use of these modules, we believe the impact is restricted due to the fact that EOS-based products and WI-FI AP are usually running on customer's management networks and are not reachable from the public Internet.

A current list of affected products is included below and Arista and will update this advisory with information pending ongoing assessment.

Vulnerability Assessment

Affected Software

Please consult the section on Required Configuration for Exploitation if products are found which are affected. Specific configuration is necessary for this vulnerability to impact the product.

The following product releases are affected by CVE-2023-45288:

Streaming Telemetry Agent (TerminAttr) versions:

- 1.30.0
- 1.29.0
- 1.28.3 and below releases in the 1.28.X train
- 1.27.0
- 1.26.0
- 1.25.1 and below releases in the 1.25.X train
- 1.24.3 and below releases in the 1.24.X train

EOS release version:

- 4.31.2F and below releases in the 4.31.x train
- 4.30.5M and below releases in the 4.30.x train
- 4.29.7M and below releases in the 4.29.x train
- 4.28.10.1M and below releases in the 4.28.x train
- 4.27.12M and below releases in the 4.27.x train

- 4.26.13M and below releases in the 4.26.x train

WI-FI Access Points versions:

- 16.1 and below releases

The following product releases are affected by CVE-2024-28182:

Awake Security versions

- 5.1.2 and below releases in the 5.1.x train
- 5.0.6 and below releases in the 5.0.x train
- 4.2.5 and below releases in the 4.2.x train

Affected Platforms

Please consult the section on Required Configuration for Exploitation if products are found which are affected. Specific configuration is necessary for this vulnerability to impact the product.

The following product platforms are affected by CVE-2023-45288:

- 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 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
    - All AP models

The following product platforms are affected by CVE-2024-28182:

- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
    - Arista NDR AVA Nucleus
    - Arista NDR AVA Campus Nucleus

The following cloud services have mitigated CVE-2024-30255:

- CloudVision CUE cloud service delivery
- CloudVision as-a-Service

The following products are currently under investigation:

- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
    - Cloud-hosted: NDR Analyst Portal

The following products are not affected by any HTTP/2 vulnerabilities listed above:

- Arista EOS-based products not using the EOS affected feature list mentioned in the description section
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision eXchange, virtual or physical appliance
- CloudVision AGNI
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
    - Arista NDR Central Console
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics

Required Configuration for Exploitation

CVE-2023-45288

Arista EOS-based products

Prerequisites for CVE-2023-45288 are that the EOS affected feature list mentioned in the description section are enabled on the device.

Streaming Telemetry Agent is enabled on the device and configured for gRPC/gNMI access (not common for CloudVision deployments):

```
daemon TerminAttr
   exec /usr/bin/TerminAttr -grpcaddr=... <other options...>
   no shutdown
```

Note: the TerminAttr flag “-grpcaddr” is not enabled by default and is used to serve data using the gNMI interface, which is not common for CloudVision deployments. The flag must be configured specifically to be vulnerable to CVE-2023-45288.

OpenConfig gNMI is enabled on the device:

```
management api gnmi
   transport grpc <name>
```

gRIBI is enabled on the device:

```
management api gribi
   transport grpc <name>
```

Octa is enabled on the device:

```
management api gnmi
   provider eos-native
```

Arista Wireless Access Points

The prerequisite for CVE-2023-45288 is that the OpenConfig flag is enabled on Access Point. Please contact the TAC team to understand the support for OpenConfig on the devices.

CVE-2024-28182

Arista Awake NDR

NDR Ava Nucleus and NDR Ava Campus Nucleus can be exploited with the vulnerability by default.

Indicators of Compromise

Successful exploitation of this vulnerability can allow an attacker the capability to launch DoS attacks against servers or cause an out of memory (OOM) crash. Therefore the unusually slow network performance, unavailability of a particular website or a sudden loss of connectivity across devices on the same network can be used as indicators of the compromise for the vulnerabilities.

Mitigation

CVE-2023-45288

Arista EOS-based products

As a security best practice, it is recommended to not expose internal devices to public access to safeguard from potential attacks. There are 2 possible options to mitigate the vulnerability on the EOS products as listed below

Configure Access-Control List to restrict access

Configure a non-default Control-Plane ACL to restrict traffic from trusted sources on service ports :

```
permit tcp 10.10.10.0/24 any eq 6042
```

In this example, connections to port 6042 (Streaming Telemetry Agent's default gRPC/gNMI port) will only be accepted if sourced from the 10.10.10.0/24 subnet.

The following are the default service ports for the affected features:

- gRIBI - 6040
- OpenConfig and Octa - 6030
- TerminAttr - 6042

For OpenConfig, Octa and gRIBI, an alternative solution is to configure a service ACL to restrict incoming traffic.

First configure a service ACL to only allow HTTP/2 traffic from trusted sources.

```
ip access-list standard grpc-acl
   10 permit host 10.1.1.1
   20 permit host 11.1.1.1/24
```

In this example, HTTP/2 connections will only be accepted if sourced from 10.1.1.1 or 11.1.1.1/24 subset.

Then configure the service ACL to the affected feature agents.

For Openconfig:

```
management api gnmi
   transport grpc default
      ip access-group grpc-acl
```

For Octa:

```
management api gnmi
   transport grpc default
      ip access-group grpc-acl
   provider eos-native
```

For gRIBI:

```
management api gribi
   transport grpc default
      ip access-group grpc-acl
```

Enforce mTLS for authentication

First create an SSL profile using the certificate. For more details on certificate generation and EOS-based product SSL profile management, please refer to the article Working with certificates.

```
management security
   ssl profile mtls-grpc-profile
```

```
      certificate target.crt key target.key
      trust certificate ca.crt
```

For Streaming Telemetry Agent, specify the certificate and key file used by gNMI server

```
daemon TerminAttr
   exec /usr/bin/TerminAttr
      -certfile /persist/secure/ssl/certs/target.crt
      -keyfile /persist/secure/ssl/keys/target.key
      -clientcafile /persist/secure/ssl/certs/ca.crt
   no shutdown
```

For Openconfig:

```
management api gnmi
   transport grpc default
      ssl profile mtls-grpc-profile
```

For Octa:

```
management api gnmi
   transport grpc default
      ssl profile mtls-grpc-profile
   provider eos-native
```

For gRIBI:

```
management api gribi
   transport grpc default
      ssl profile mtls-grpc-profile
```

Arista Wireless Access Points

There is no mitigation available to temporarily resolve the issue when Openconfig is enabled

CVE-2024-28182

Arista Awake NDR

There is no mitigation available to temporarily resolve the issue

Resolution

CVE-2023-45288

Arista EOS-based products

There are no fixes presently available for affected products.

Arista Wireless Access Points

There are no fixes presently available for affected products.

CVE-2024-28182

Arista Awake NDR

There are no fixes presently available for affected products.

Note: For products presently without available fixes, please review this document periodically for updates

References

- https://kb.cert.org/vuls/id/421644
- https://nowotarski.info
- https://nvd.nist.gov/vuln/detail/CVE-2023-45288
- https://nvd.nist.gov/vuln/detail/CVE-2024-2653
- https://nvd.nist.gov/vuln/detail/CVE-2024-27316
- https://nvd.nist.gov/vuln/detail/CVE-2024-2758
- https://nvd.nist.gov/vuln/detail/CVE-2024-27919
- http://nvd.nist.gov/vuln/detail/CVE-2024-27983
- https://nvd.nist.gov/vuln/detail/CVE-2024-28182
- http://nvd.nist.gov/vuln/detail/CVE-2024-30255
- http://nvd.nist.gov/vuln/detail/CVE-2024-31309

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