Date: May 27th, 2022

Revision	Date	Changes
1.1	May 27th 2022	Update the CVE impact of Octa
1.0	May 25th 2022	Initial release

CVE-2021-28508

- CVSSv3.1 Base Score: 6.8 (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H)
- CWE: CWE-255 Credentials Management Errors
- Tracking bug: BUG635204 (TerminAttr), BUG664159 (Octa)

CVE-2021-28509

- CVSSv3.1 Base Score: 6.1 (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N)
- CWE: CWE-255 Credentials Management Errors
- Tracking bug: BUG643445 (TerminAttr), BUG664160 (Octa)

Description

This advisory documents the impact of an internally found vulnerability in Arista EOS state streaming telemetry agent TerminAttr and OpenConfig transport protocols.

The impact of this vulnerability is that, in certain conditions, TerminAttr or Octa might leak IPsec (CVE-2021-28508) and MACsec (CVE-2021-28509) sensitive data in clear text to CloudVisions's authorized users or authorized gNMI clients. The leaked data could allow IPsec and MACsec traffic to be decrypted or modified.

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

Vulnerability Assessment

Affected Software

CVE-2021-28508

EOS versions (When Octa is in use on the device) :

- 4.23.11 and below release in the 4.23.x train
- 4.24.9 and below release in the 4.24.x train
- 4.25.7 and below releases in the 4.25.x train
- 4.26.5 and below releases in the 4.26.x train
- 4.27.1 and below releases in the 4.27.x train

TerminAttr versions:

- TerminAttr v1.10.10 and all prior releases
- TerminAttr v1.16.7 and all prior releases in the v1.11.x-v1.16.x trains
- TerminAttr v1.18.1 and all prior releases in the v1.17.x-v1.18.x trains

CVE-2021-28509

EOS versions (When Octa is in use on the device) :

- 4.23.11 and below release in the 4.23.x train
- 4.24.9 and below release in the 4.24.x train
- 4.25.7 and below releases in the 4.25.x train
- 4.26.5 and below releases in the 4.26.x train
- 4.27.3 and below releases in the 4.27.x train

TerminAttr versions:

- TerminAttr v1.10.10 and all prior releases
- TerminAttr v1.16.7 and all prior releases in the v1.11.x-v1.16.x trains
- TerminAttr v1.19.1 and all prior releases in the v1.17.x-v1.19.x trains

Affected Platforms

All EOS-based platforms that support IPsec or MACsec with the versions identified above are affected with TerminAttr or Octa enabled on the device.

Arista EOS-based products that support IPsec:

- DCS-7020SRG
- DCS-7280CR3MK

Arista EOS-based products that support MACsec:

- 722XP series
- 7050X3 series
- 7280R/R2/R3 series
- 7388X5 series

- 7500R/R2/R3 series
- 7800R3 series

The following products are **not** affected:

- Arista EOS-based products:
    - 710P series
    - 750X series
    - 7010/X series
    - 7050X/X2/X4 series
    - 7060X/X2/X4 series
    - 7130 series
    - 7150 series
    - 7160 series
    - 7170 series
    - 7250X series
    - 7260X/X3 series
    - 7300X series
    - 7320X series
    - 7358X4 series
    - 7368X4 series
    - 7388X5 series
- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Awake Security Platform

Required Configuration for Exploitation

The prerequisite for both CVEs is that TerminAttr or Octa is enabled on the device

TerminAttr is enabled on the device:

```
daemon TerminAttr
   exec /usr/bin/TerminAttr ...
   no shutdown
```

Octa is enabled on the device:

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

CVE-2021-28508

IPsec is configured on device:

```
ip security
   profile Arista
      ike-policy ikedefault
      sa-policy sadefault
      connection start
      shared-key 7 047A190F1C354D
      mode transport
```

CVE-2021-28509

MACsec is configured on device:

```
mac security
   profile Arista
      key 0abc1234 7 06070E234E4D0A48544540585F507E
      key 0def5678 7 09484A0C1C0311475E5A527D7C7C70 fallback

interface Ethernet6/1
   mac security profile Arista
```

Indicators of Compromise

TerminAttr

When TerminAttr is used directly on the device to stream, check if TerminAttr is running with the affected version mentioned above.

To check the installed TerminAttr version on the system, use the following command:

```
#show version detail | grep TerminAttr-core
TerminAttr-core      v1.13.3         1
```

To check if TerminAttr is running, use the following command and make sure there's a PID allocated to the process:

```
#show daemon TerminAttr
Process: TerminAttr (running with PID 2430)
```

Octa

When Octa is used on the device to stream for OpenConfig modeled data and "eos-native" data over the gNMI, check if Octa is enabled on the device.

To check if Octa is running on the device, use the following show command to check Octa status:

```
#show management api gnmi
Octa:                enabled
Enabled:             Yes
Server:              running on port 6030, in default VRF
SSL Profile:         none
QoS DSCP:            none
```

Mitigation

The following configuration changes may be made in order to mitigate the exploitation of the listed vulnerability.

On the affected versions, the vulnerabilities can be mitigated by disabling the streaming agent in use on the device.

TerminAttr

```
daemon TerminAttr
```

```
   shutdown
```

Octa

```
management api gnmi
   no provider eos-native
```

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience.

CVE-2021-28508

The vulnerability is fixed in the following versions:

EOS versions: (When Octa is in use on the device) :

- 4.24.10 and later release in the 4.24.x train
- 4.25.8 and later releases in the 4.25.x train
- 4.26.6 and later releases in the 4.26.x train
- 4.27.2 and later releases in the 4.27.x train

TerminAttr versions:

- TerminAttr v1.10.11 and later releases in the v1.10.x train
- TerminAttr v1.16.8 and later releases in the v1.16.x train
- TerminAttr v1.19.0 and later releases

CVE-2021-28509

The vulnerability is fixed in the following versions:

EOS versions (When Octa is in use on the device) :

- 4.24.10 and later release in the 4.24.x train
- 4.25.8 and later releases in the 4.25.x train
- 4.26.6 and later releases in the 4.26.x train
- 4.27.4 and later releases in the 4.27.x train

TerminAttr versions:

- TerminAttr v1.10.11 and later releases
- TerminAttr v1.16.8 and later releases in the v1.11.x-v1.16.x trains
- TerminAttr v1.19.2 and later releases in the v1.17.x-v1.19.x trains

As mentioned above, TerminAttr has been bundled with every EOS release from 4.17.0F and above and it's also available as a SWIX extension that can be used to upgrade TerminAttr to the latest version independently. For instructions on upgrading TerminAttr to the fixed release from CLI on EOS-based products, please refer to the article TerminAttr – Upgrade & Downgrade.

An EOS upgrade is required only when Octa is in use.

Hotfix

No hotfix is available for these CVEs.

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