**Date: September 28th 2023**

| Revision | Date | Changes |
|---|---|---|
| 1.5 | September 28th 2023 | Update to include 4.29 to EOS Releases that resolve the CVE's |
| 1.4 | January 11th 2023 | Update the fixed release info of NetVisor OS Software |
| 1.3 | October 24th 2022 | Update the fixed release info |
| 1.2 | October 7th 2022 | Update the mitigation configuration |
| 1.1 | September 29th 2022 | Update the fixed release info and required configuration |
| 1.0 | September 27th 2022 | Initial release |

**This security advisory addresses four CVEs:**

- **CVE-2021-27853**
    - CVSSv3.1 Base Score: 4.7( CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N )
    - CWE: CWE-290 Authentication Bypass by Spoofing
    - Tracking Bug: BUG615000 (EOS) and PR45661(NetVisor)
- **CVE-2021-27854**
    - CVSSv3.1 Base Score: 4.7( CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N )
    - CWE: CWE-290 Authentication Bypass by Spoofing
    - Tracking Bug: BUG682330
- **CVE-2021-27861**
    - CVSSv3.1 Base Score: 4.7( CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N )
    - CWE: CWE-290 Authentication Bypass by Spoofing
    - Tracking Bug: BUG615000 (EOS) and PR45661(NetVisor)
- **CVE-2021-27862**
    - CVSSv3.1 Base Score: 4.7( CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N )
    - CWE: CWE-290 Authentication Bypass by Spoofing
    - Tracking Bug: BUG682330

## Description

This advisory documents the impact of 4 publicly disclosed vulnerabilities within Ethernet encapsulation protocols on Arista products. These issues affect multiple networking vendors

and the coordination of this disclosure has been handled by IEEE. Affected Arista products include EOS systems, Wi-Fi Access Points and NetVisor OS Software. The affected software releases are listed below.

The issues involve how L2 network security controls can be bypassed using VLAN 0 stacking (hereby referred to as the “VLAN 0 header stack variant”) or 802.3 LLC headers with invalid length (hereby referred to as the “LLC Header Invalid Length Variant”). An attacker can send crafted packets through vulnerable devices to cause Denial-of-Service (DoS) or to perform a Man-in-the-Middle (MitM) attack against L2 reachable hosts in the network.

These issues are tracked via the following four CVEs:

- CVE-2021-27853: Layer 2 network filtering capabilities such as IPv6 RA guard or ARP inspection can be bypassed using combinations of VLAN 0 headers and LLC/SNAP headers.
- CVE-2021-27854: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using combinations of VLAN 0 headers, LLC/SNAP headers in Ethernet to Wifi frame translation and the reverse Wifi to Ethernet.
- CVE-2021-27861: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length (and optionally VLAN0 headers).
- CVE-2021-27862: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length and Ethernet to Wifi frame conversion (and optionally VLAN0 headers).

As of the time of this publication, Arista is not aware of any malicious uses of this issue in customer networks.

## Vulnerability Assessment

### Affected Software

#### CVE-2021-27853 and CVE-2021-27861

- EOS Versions
    - 4.28.2F and older releases in the 4.28.x train
    - 4.27.6M and older releases in the 4.27.x train
    - 4.26.7M and older releases in the 4.26.x train
    - 4.25.9M and older releases in the 4.25.x train
    - 4.24.10M and older releases in the 4.24.x train
    - 4.23.12M and older releases in the 4.23.x train
    - 4.22.12M and older releases in the 4.22.x train
    -
- Wi-Fi Access Points
    - 12.0.1-48 and older releases for the 12.0 train
    - 11.0.1-49 and older releases for the 11.0 train

    - 10.0.1-31 and older release for the 10.0 train
    -
- NetVisor OS Versions

    - 7.0.2 GA and older releases in the 7.x.x train
    - 6.1.2 HF1 and older releases in the 6.x.x train (ONIE)
    - 6.1.1 HF7 and older releases in the 6.x.x train (non-ONIE)
    - 5.2.1 HF4 and older releases in the 5.x.x train
    -

#### CVE-2021-27854 and CVE-2021-27862

- Wi-Fi Access Points

    - 12.0.1-48 and older releases for the 12.0 train
    - 11.0.1-49 and older releases for the 11.0 train
    - 10.0.1-31 and older release for the 10.0 train

**NOTE:** Both a vulnerable network device and a vulnerable host networking stack must be present for the issues to be exploitable. Thus, in addition to network devices, it is strongly recommended to evaluate the exposure of the IP stack of connected hosts for a complete assessment of these vulnerabilities.

## Affected Platforms

#### CVE-2021-27853 and CVE-2021-27861

### Platforms impacted by VLAN 0 Header Stack Variant

- Arista EOS Based products

    - 7010 and 7010X series
    - 7020R series
    - 7050X/X2/X3/X4 series
    - 7060X/X2/X4 series
    - 7150 series
    - 7160 series
    - 7170 series
    - 710P series
    - 720XP series
    - 722XPM series
    - 750X series
    - 7250X series
    - 7260X/X3 series
    - 7280E/R/R2 series
    - 7280R3 series
    - 7300X/X3 series

    - 7320X series
    - 7358X4 series
    - 7368X4 series
    - 7388X5 series
    - 7500E/R/R2 series
    - 7500R3 series
    - 7800R3 series
    -
- Wi-Fi Access Points
    - 11ac wave-2 Access Point series (C100, C110, W118, C120, C130, O105 and their variants)
    - 11ax (Wi-Fi6) Access Point series (C200, C230, O235, C250, C260, C360 and their variants)
    -
- All NetVisor OS-based products
    - AS5712 series
    - AS5812 series
    - AS5835 series
    - AS6712 series
    - AS7312 series
    - AS7316 series
    - AS7326 series
    - AS7712 series
    - AS7716 series
    - AS7726 series
    - AS7816 series
    - Freedom 9K series
    - NSU series
    - NRU01 series
    - NRU02 series
    - NRU03 series
    - S52xx series
    - S5048 series
    - S60xx series
    - S41xx series
    - S40xx series
    - Z9264 series
    - Z9100 series
    - AS5712 series
    - AS6712 series
    - AS7316 series
    - AS7716 series
    - S60xx series
    - S40xx series

### Platforms impacted by LLC Header Invalid Length Variant

- Arista EOS Based products
    - 7010 and 7010X series
    - 7050X/X2/X3/X4 series
    - 7060X/X2/X4 series
    - 7150 series
    - 7160 series
    - 7170 series
    - 710P series
    - 720XP series
    - 722XPM series
    - 750X series
    - 7250X series
    - 7260X/X3 series
    - 7280R3 series
    - 7300X/X3 series
    - 7320X series
    - 7358X4 series
    - 7368X4 series
    - 7388X5 series
    - 7500R3 series
    - 7800R3 series
    -
- Wi-Fi Access Points
    - 11ac wave-2 Access Point series (C100, C110, W118, C120, C130, O105 and their variants)
    - 11ax (Wi-Fi6) Access Point series (C200, C230, O235, C250, C260, C360 and their variants)
    -
- All NetVisor OS-based products
    - AS5712 series
    - AS5812 series
    - AS5835 series
    - AS6712 series
    - AS7312 series
    - AS7316 series
    - AS7326 series
    - AS7712 series
    - AS7716 series
    - AS7726 series
    - AS7816 series
    - Freedom 9K series
    - NSU series

    - NRU01 series
    - NRU02 series
    - NRU03 series
    - S52xx series
    - S5048 series
    - S60xx series
    - S41xx series
    - S40xx series
    - Z9432 series
    - Z9264 series
    - Z9100 series
    - AS5712 series
    - AS6712 series
    - AS7316 series
    - AS7716 series
    - S60xx series
    - S40xx series

**CVE-2021-27854 and CVE-2021-27862**

- Wi-Fi Access Points
    - 11ac Wave-2 Access Point series (C100, C110, W118, C120, C130, O105 and their variants)
    - 11ax (Wi-Fi 6) Access Point series (C200, C230, O235, C250, C260, C360 and their variants)

The following product versions and platforms are not affected by any of the listed CVEs

- ClouldEOS and vEOS Router
- CloudVision Wi-Fi, virtual appliance or physical appliance
- CloudVision Wi-Fi cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- Arista 7130 Systems running MOS or EOS
- Arista Converged Cloud Fabric (CCF) and DANZ Monitoring Fabric (DMF) (Formerly Big Switch Nodes for BCF and BMF)
- Awake Security Platform
- NG Firewall and Micro Edge

The following products are not affected by LLC Variant of CVE-2021-27853 and CVE-2021-27861 but are still affected by the VLAN 0 Header Stack Variant

- 7020R Series
- 7280E/R/R2 series
- 7500E/R/R2 series

## Required Configuration for Exploitation

### CVE-2021-27853 and CVE-2021-27861

### EOS Configuration

Any of the following L3 aware L2 security filtering features is in use:
**ACLs configured on Ethernet ports, Port-Channels or VLANs**

```
ip access-group <aclName> in
ipv6 access-group <aclName> in
```

### IP Locking feature family

```
(config-if-EtX)# address locking ipv4
(config-if-EtX)# address locking ipv6
(config-if-EtX)# address locking ipv4 ipv6

in conjunction with
(config-address-locking)# dhcp server ipv4 <A.B.C.D>
(config-address-locking)# local-interface <interface>
and/or
(config-address-locking)# locked-address [ipv4|ipv6] enforcement disabled
```

### ARP Inspection

```
ip arp inspection
```

### Interface Traffic Policies

```
(config-if-EtX/Y)#traffic-policy input <traffic-policy-name>
```

### Segment Security Policies

```
(config)#router segment-security
(config-router-seg-sec)#no shutdown
```

#### Wi-Fi Access Point Configuration

SSID Firewall rules matching L3 and L4 headers

#### NetVisor OS Configuration

Any of the following L3 aware L2 security filtering features is in use:
Security and QoS based vFlows configured on Ethernet ports, trunks, or VLANs

```
CLI> vflow-create name L3-vflow scope local src-ip 1.1.1.1/24 dst-
ip 1.1.1.2/24 action drop
```

IPv6 RA Guard requires creation of a filter for addresses and prefixes to apply a security profile to RA messages

```
CLI> access-list-create name list1 scope local
CLI> access-list-ip-add name list1 ip fe80::640e:94ff:fe29:b4d0
CLI> ipv6security-raguard-create name ra1 device router access-list list1
CLI> ipv6security-raguard-port-add name ra1 ports 37
```

#### CVE-2021-27854 and CVE-2021-27862

#### Wi-Fi Access Point Configuration

SSID Firewall rules matching L3 and L4 headers

## Indicators of Compromise

There are no visible indicators of compromise.

## Mitigation

### EOS Based Products

The mitigations below are supported on all the EOS platforms (except the 7170 series) in the affected releases.

To mitigate the VLAN 0 header stack variant vulnerability, the following MAC ACL can be configured.

```
mac access-list Vlan0HeaderVariant
   deny any any 0x8100
   deny any any 0x88a8
   permit any any
```

Whenever the switch is unable to resolve the final protocol ethertype of an Ethernet frame with a VLAN tag sequence, the final ethertype is determined to be one of the known VLAN tag ethertypes (Tag Protocol ID or TPID) 0x8100 or 0x88a8. The ‘Vlan0HeaderVariant’ ACL causes such frames to be discarded.

To mitigate the LLC header invalid length variant vulnerability, the following MAC ACL such as the sample below can be configured

```
mac access-list allowSpecificEtypes
   permit any any ip
   permit any any ipv6
   permit any any arp
   deny any any
```

The ‘allowSpecificEtypes’ ACL provides protection against both variants by ensuring that a switch is allowed to forward a packet only if it is successfully able to identify a higher layer protocol in use in the packet header behind a sequence of VLAN tags. This ACL functions as a permit list to allow known good ethertypes through and drops everything else. This means that all higher layer protocol ethertypes being used in a network have to be identified and included in the permit list to ensure connectivity for those protocols.

**Note: The TPID ethertype values 0x8100 and 0x88a8 must not be included in the permit list. The switch will only identify the ethertype of a frame as one of these values only if it encounters a VLAN tag sequence that is long enough that it is unable to parse and derive a final ethertype.**

Once a suitable ACL is constructed, it must be applied on all L2 switch ports connected to uncontrolled hosts.

```
(config)#interface etX/Y
(config-if-EtX/Y)#mac access-group <mitigationAclName> in
```

## Wi-Fi Access Point

There are no known mitigations for Wi-Fi access points.

## NetVisor OS

There are no known mitigations for NetVisor OS Software.

## 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 software release that contains all the fixes listed below.

## EOS Releases that resolve the CVEs

#### CVE-2021-27853 and CVE-2021-27861

- 4.29 and later releases
- 4.28.3M and later releases in the 4.28.x train
- 4.27.7M and later releases in the 4.27.x train
- 4.26.8M and later releases in the 4.26.x train
- 4.25.10M and later releases in the 4.25.x train
- 4.24.11M and later releases in the 4.24.x train
- 4.23.13M and later releases in the 4.23.x train
- 4.22.13M and later releases in the 4.22.x train

### Post Upgrade Steps

The following global commands MUST be enabled on all fixed releases to resolve the vulnerabilities.

To fix the VLAN 0 header stack variant vulnerability

```
switchport vlan tag validation
```

To fix the LLC header variant vulnerability

```
switchport ethernet llc validation
```

Only platforms which are affected by a variant will be able to run the corresponding configuration command to resolve the issue. Cross reference your platform with the affected variant (Affected Platforms section above) to determine the configuration command(s) which should be set. A configuration command which does not apply to the platform will be unavailable on that platform.

## Wi-Fi Access Point Software Releases that resolve the CVEs

#### CVE-2021-27853, CVE-2021-27854, CVE-2021-27861 and CVE-2021-27862

- 12.0.1-48.20 and later releases for the 12.0.1 train

- 11.0.1-49.16 and later releases for the 11.0.1 train

**Note:** all releases in the 10.0 train are affected by the CVEs. Please upgrade to the fixed release versions in 11.0.1 or 12.0.1 train as soon as possible. If you require further assistance, please contact the Arista Networks Technical Assistance Center (TAC) with methods listed below.

### Post Upgrade Steps

There are no post upgrade steps required for Wi-Fi.

## NetVisor OS Releases that resolve the CVEs

### CVE-2021-27853 and CVE-2021-27861

- 7.0.2 HF1 and later releases in the 7.x.x train
- 6.1.2 HF2 and later releases in the 6.x.x train (ONIE)
- 6.1.1 HF8 and later releases in the 6.x.x train (non-ONIE)
- 5.2.1 HF5 and later releases in the 5.x.x train

For details on upgrading NetVisor OS releases, refer to "Upgrading the NetVisor OS Software" section in the respective Release Notes documentation.

### Post Upgrade Steps

The following global commands MUST be enabled to resolve the vulnerabilities.

**Note:** Prior to enabling the below CLI command options, ensure that there are no error messages while creating new vFlows such as the below, the messages are also available in the nvOSd.log file.

```
vflow-create: Flow Table System-L1-L4-Tun-1-0 is Full
```

To fix the VLAN 0 header stack variant vulnerability

```
CLI> system-settings-modify vlan-tag-validate
```

This option is disabled by default. And when you enable this option using the above command, NetVisor OS automatically creates 5 vFlows upon switch reboot with appropriate precedence values and drops the double-tagged and triple-tagged packets.

To fix the LLC header variant vulnerability

```
CLI> system-settings-modify l2-frame-validate
```

This option is disabled by default. And when you enable this option, NetVisor OS automatically creates 5 vFlows upon switch reboot with appropriate precedence values and drops the invalid LLC/SNAP packets and bypasses the legitimate LLC/SNAP packets.

**Note:** On platforms where the virtual Link Extension (vLE) and virtual port groups (vPG) are configured, it is recommended not to enable the **l2-frame-validate** option as it may not bypass the L2 protocol packets.

To verify if the validation settings have been successfully configure

```
CLI> system-settings-show format l2-frame-validate, vlan-tag-validate
l2-frame-validate: on
vlan-tag-validate: on
```

**Note:** Reboot the switch after making (enable/disable) the above configurations for the changes to take effect.

To allow Q-in-Q packet match on L3 IP header, enable **allow-tpid**

```
CLI> port-config-modify port <logical port number> allowed-tpid vlan,q-in-q,q-in-q-old,
```

When the above parameter is enabled, the **system-settings-modify vlan-tag-validate** command and the **system-settings-modify l2-frame-validate** command adds 5 vFlows each upon switch reboot.

### Hotfix

There is no hotfix available for any of the affected platforms.

## References

- https://kb.cert.org/vuls/id/855201
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27853
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27854
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27861
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27862

## 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