Date:December 16th, 2020

Version: 1.0

Revision	Date	Changes
1.0	December 16th, 2020	Initial Release

The CVE-ID tracking this issue is: CVE-2020-3702
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

Description

This advisory documents the impact of a vulnerability in the 2.4GHz radios of Arista Wireless Access Points (APs). Not all systems are impacted, please refer to the “Affected Platforms”, and “Symptoms” sections below for specific required configuration to be vulnerable.

The effect of this vulnerability is that, under certain conditions, APs configured to use the WPA2 or the WPA/WPA2 mixed-mode encryption standards may temporarily transmit Wi-Fi traffic without encryption. Please note that Wi-Fi traffic which is encrypted at higher layers (ex. a TLS connection) by edge devices (ex. desktops, phones etc.) will remain encrypted by the application layer’s encryption.

This vulnerability is applicable if all of the following conditions are matched:

- The AP is performing an encryption of Wifi traffic using the WPA2 or WPA/WPA2 mixed-mode security standards.
- The Wifi traffic in question is bridged using the 2.4GHz radio of the Access Point i.e. there are active SSIDs configured for the 2.4GHz band with edge devices connected to the same.
- The Access Point model is present in the list of Affected Platforms below.

Details on how to determine if these settings apply can be found under “Symptoms”.

This vulnerability is NOT applicable if any one (or more) of the following conditions are matched:

- The AP is performing an encryption of Wi-Fi traffic using the WEP standard.
- Wi-Fi traffic is bridged using the 5.0Ghz radio of the Access Point alone i.e. there is no traffic bridged using the 2.4GHz radio or the SSID(s) of the 2.4GHz radio has been disabled.
- The AP model is not present in the list of Affected Platforms below.

Arista is not aware of any malicious uses of this issue in customer networks.

Symptoms

The following checks can be performed on the AP to determine if this vulnerability is applicable.

1) Confirm the AP model.

- Login to the CloudVision Wifi GUI.
- Navigate to Monitor -> Wifi -> Access Points.
- Observe the Access Point model under the “Model” column (Highlighted in orange):

Example:

Access Points

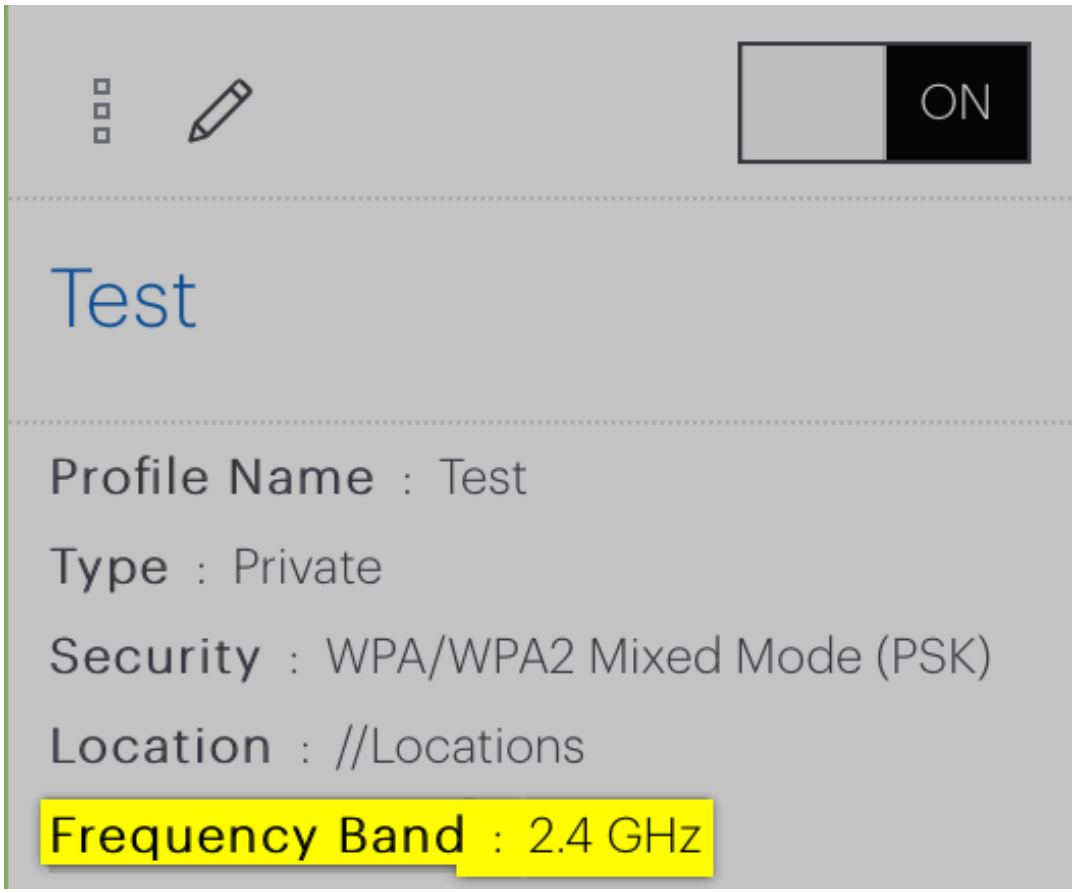
Status	Name	Last Booted At	No. of Associations	Power Source	Capability	Model
	Arista_B0:03:5F	Oct 17	--	PoE+	802.11n/ac/ax, AP	C-260
	Arista_C0:08:0F	Oct 17	--	PoE+	802.11n/ac/ax, AP	C-230
	Arista_A0:1B:BF	Oct 17	--	DC	802.11n/ac/ax, AP	C-250
	Arista_D4:F2:BF	Oct 16	--	--	802.11n/ac, AP	C-75

Note: Please refer to the “Affected Platforms” section below for the list of affected models.

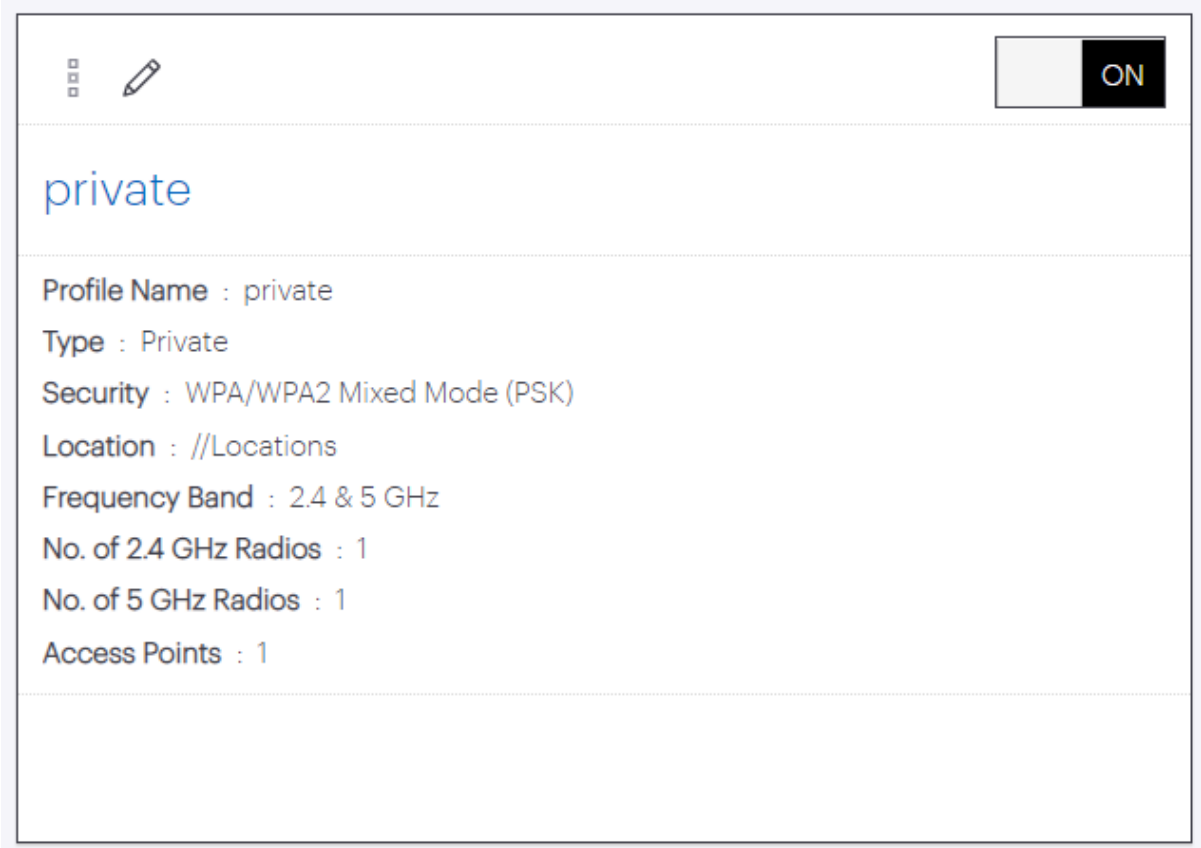
2)Confirm if a SSID(s) has been configured to operate in the 2.4GHz band.

- Login to the CloudVision Wifi GUI.
- Navigate to Configure -> SSID.
- Observe the SSID(s) configured to operate in the 2.4GHz band:

Example (GHz highlighted in yellow):



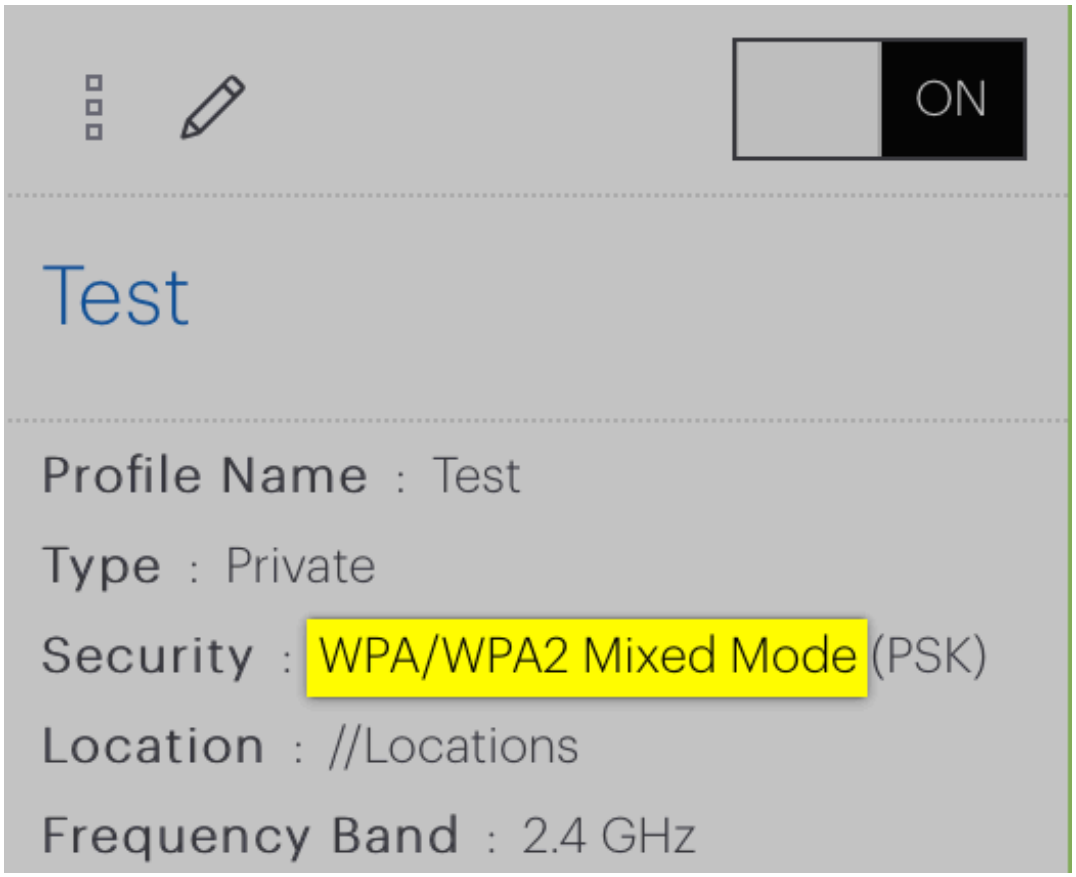
Example (The following SSID is configured to operate in both the 2.4GHz and 5 GHz bands, this is also an example of vulnerable configuration):

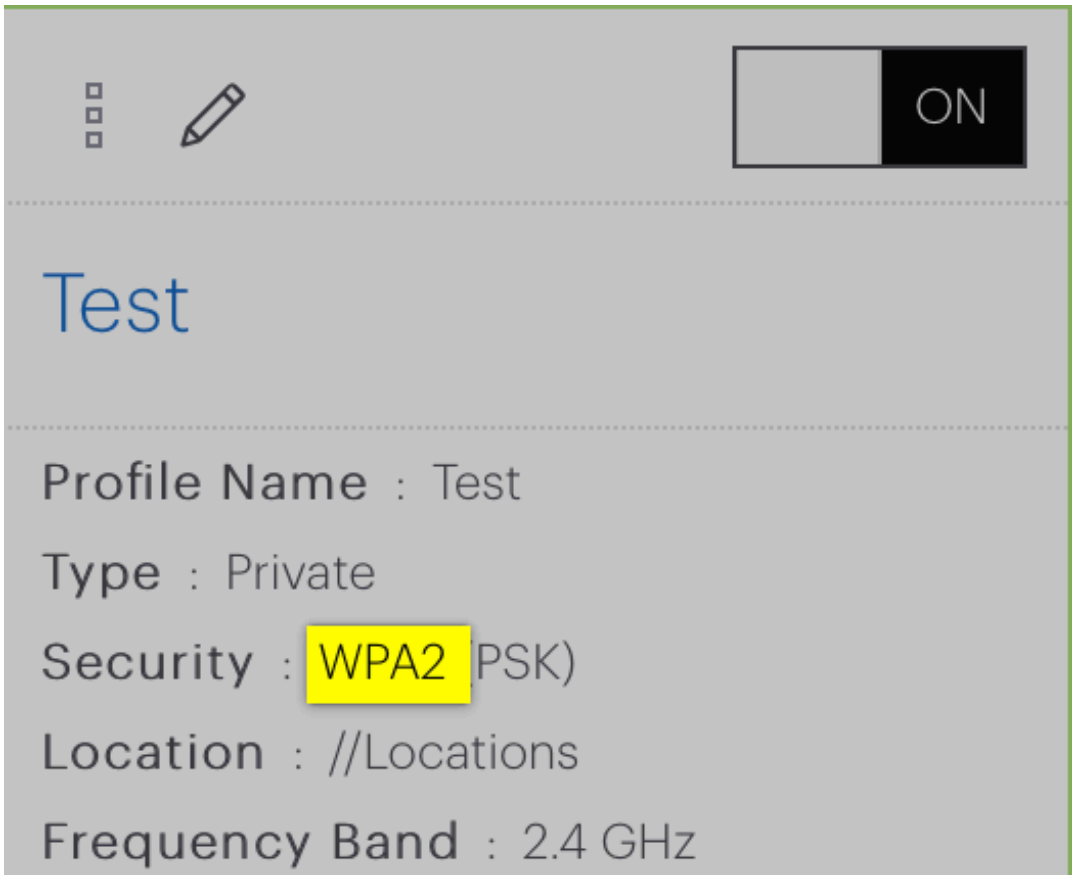


3)Confirm the encryption standard configured for the 2.4GHz SSID(s):

- Login to the CloudVision Wifi GUI
- Navigate to Configure -> SSID.
- Observe the security standard configured for the 2.4GHz SSID(s):

Example(s):



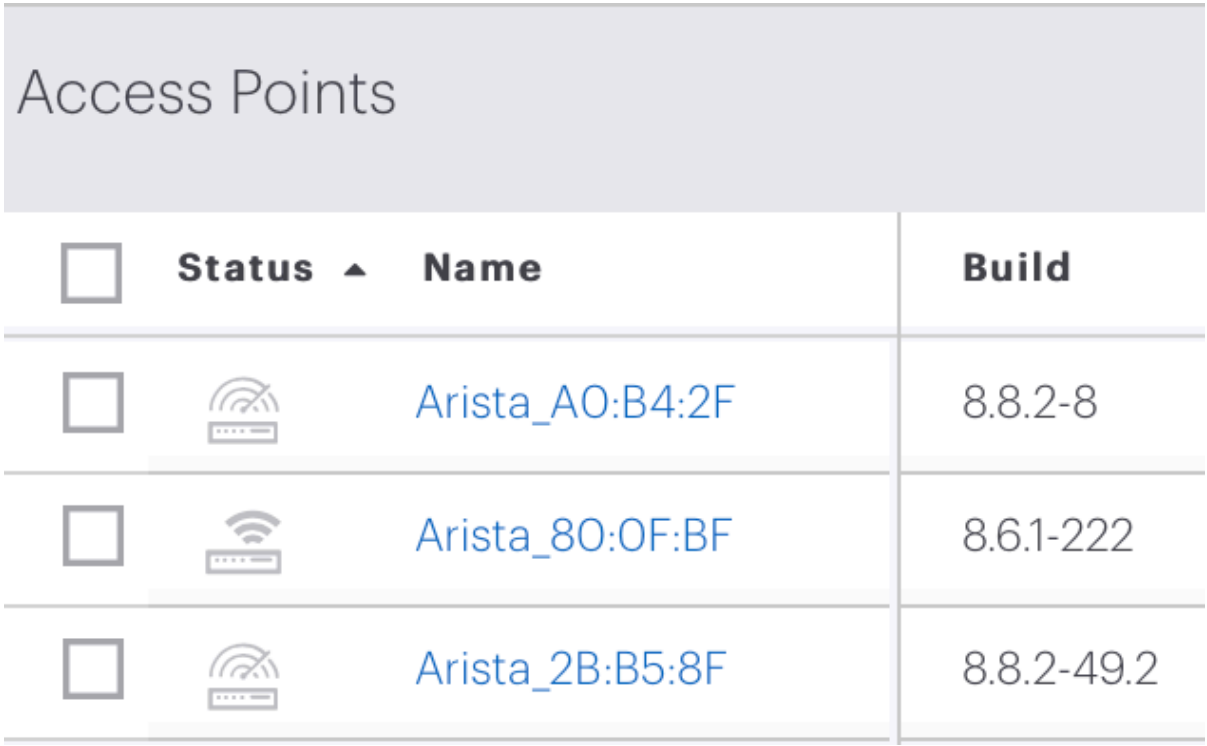


Note: As observed in the above examples, this vulnerability is applicable if either WPA2 mode or WPA/WPA2 mixed mode security standards are configured for the 2.4GHz SSID(s).

4) Confirm the AP Build version.

- Login to the CloudVision Wifi GUI.
- Navigate to Monitor -> Wifi -> Access Points.
- Observe the AP Build version under the “Build” column:

Example:



- Confirm that the build version used is one listed under the “Affected Software” section.

Vulnerability Assessment

Affected Software

- AP Build versions
  - 8.8.3-12 and below releases in the 8.8.3 train.

Affected Platforms

- This vulnerability is applicable to following Arista Wireless Access Point platforms:
  - AV2
  - C-75/C75-E
  - O-90/O90E

    - W-68

Please note that the affected AP models mentioned in the above list have reached the end of sale. However, these AP models are under active support until 2023.

- The following products are not affected:
    - Arista EOS-based products
    - Arista 7130 Systems running MOS
    - Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
    - CloudEOS Virtual Router, as a VM on-premises or in the public cloud marketplaces
    - CloudEOS Container, that runs in Kubernetes on-premises clusters
    - CloudVision WiFi, virtual appliance or physical appliance
    - CloudVision WiFi cloud service delivery
    - CloudVision Portal, virtual appliance or physical appliance
    - CloudVision as-a-Service
    - Arista Wireless Access Points:
        - C-55
        - C-60
        - C-100
        - C-110
        - C-120
        - C-130
        - C-130E
        - C-230
        - C-230E
        - C-250
        - C-260
        - O-70
        - O-105
        - O-105E
        - O-235
        - O-235E
        - W-118

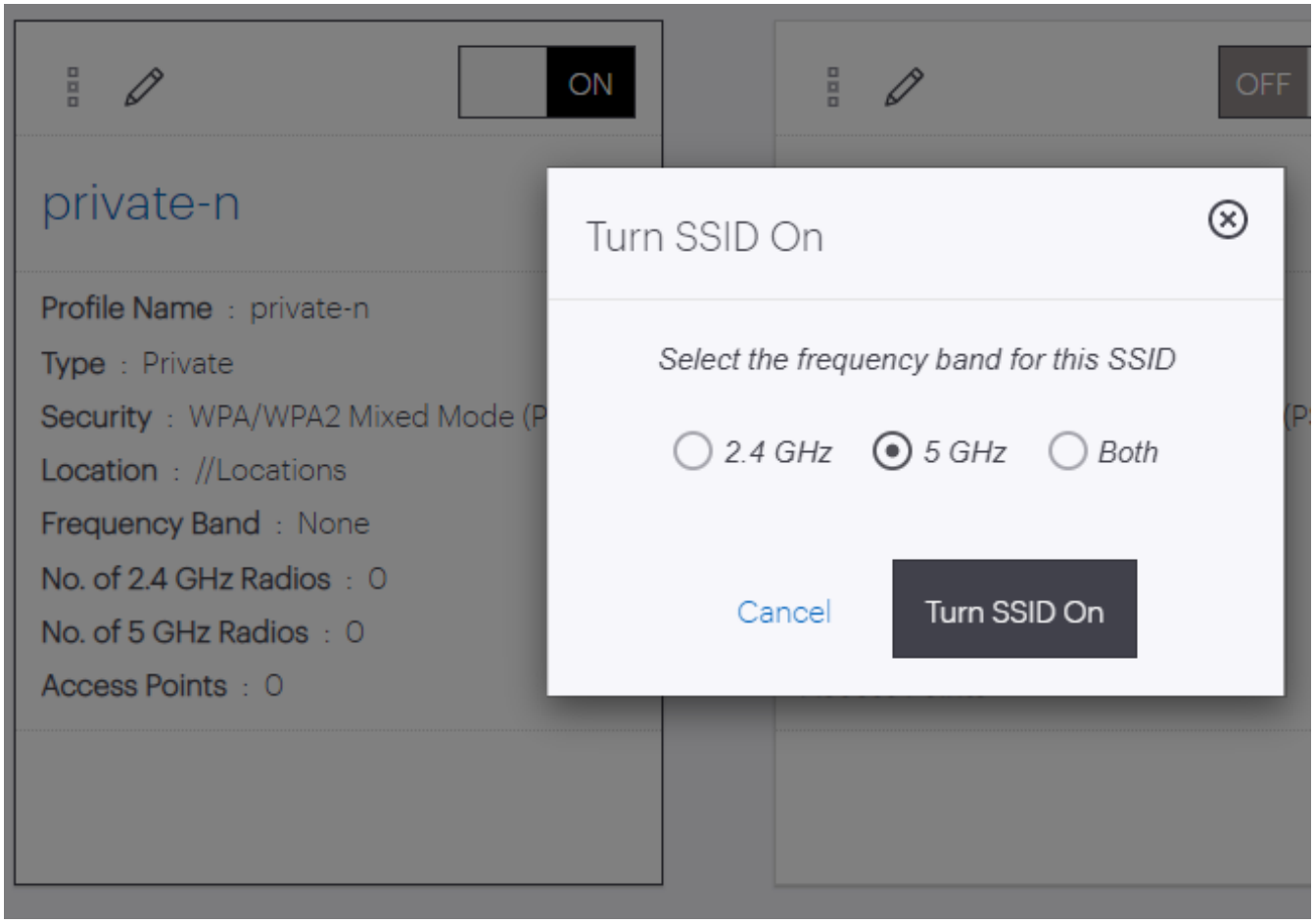
Mitigation

Any one of the following workarounds can be leveraged to mitigate the issue:

- Disable the 2.4GHz band of the SSID(s) on the affected Access Point(s). This option can be leveraged if there are dual-band (support both 2.4GHz and 5.0GHz channels) edge devices in the network, such devices can be configured to connect to the SSID(s) of the 5.0Ghz channel alone. However, single-band edge devices that operate in the 2.4Ghz band will be unable to connect to the AP if this mitigation option is used.
- To disable the 2.4GHz band of a SSID:

- Login to the CloudVision WiFi GIU
- Navigate to Configure->Wi-FI->SSID
- Select the SSID affected and turn it OFF
- Turn the SSID back on again and select “5 GHz”

Example:



- Wi-Fi traffic can be encrypted by edge devices at the application layer (ex. devices using TLS).

For the final resolution, please refer to the next section which lists the details of the remediated software versions.

Resolution

This vulnerability is being tracked by Bug 519647. The recommended resolution is to upgrade to a remediated Wi-Fi version. The vulnerability has been fixed in the following AP Build versions:

- 8.8.1-116-vv5
- 8.8.2-49-vv4
- 8.8.3-12-vv3

For instructions on how to upgrade APs, please refer to the following resources:

- On-prem deployments: https://eos.arista.com/how-to-upgrade-access-points-to-a-specific-build/
- On-prem and Cloud deployments: https://eos.arista.com/toi/cloudvision-wifi-8-8/hitless-wifi-ap-upgrades/

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