Updated: May 25th, 2021

Revision	Date	Changes
1.0	May 12th, 2021	Initial Release
1.1	May 25th, 2021	Updated assessment with impacted platforms, detection and mitigation.
1.2	June 9, 2021	Updated assessment
1.3	August 19, 2021	Updated affected platforms, fixed releases, and CVSS Scores

Description

This security advisory documents the exposure of Arista's Wi-Fi products to multiple publicly documented security vulnerabilities related to packet fragmentation and aggregation, known as Fragmentation and Forge. These vulnerabilities impact any deployments using WEP, WPA, WPA2 and WPA3 security methods with any SSID. The vulnerabilities span multiple vectors and types of attack.

The vulnerabilities are documented by Arista under Bug 561363.

CVE	Description	CVSS
CVE-2020-24586	During a connection/reconnection, fragments are cached in memory. This vulnerability can be used to inject fragmented packets; or to exfiltrate user data if the cache is accessed during the connection.	**3.5** AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N
CVE-2020-24587	When reassembling packets, the encryption key used on fragments is not required to be consistent. As a result, unrelated fragments can be mixed using valid keys. This requires a "Man in the Middle" presence level.	**2.6** AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVE-2020-24588	A payload protected wireless	**3.5**

	frame (PP A-MSDU) does not protect the Present subfield of the QoS header. As this subfield is not authenticated, the bit can be flipped to alter the aggregation status of the packet.	AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
CVE-2020-26139	During the authentication process, the AP will forward EAPOL frames, prior to sender completing authentication. Allows for packet injection into an encrypted networking during authentication.	**5.3** AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2020-26140	Plaintext data frames are accepted, despite network encryption. Allows for packet injection into an encrypted network.	**6.5** AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CVE-2020-26141	If using Temporal Key Integrity Protocol (TKIP), the Message Integrity Check (MIC) will be skipped for fragmented frames. Can be leveraged for packet injection and decryption against an encrypted network. This CVE is not applicable to the Arista Wi-Fi Solution.	NA
CVE-2020-26142	AP will treat fragmented frames as full frames. This CVE is not applicable to the Arista Wi-Fi Solution.	NA
CVE-2020-26143	Plaintext data fragments are accepted, despite network encryption. Allows for packet injection into an encrypted network.	**6.5** AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CVE-2020-26144	Plaintext A-MSDU frames are accepted on an encrypted network if the frame begins	**6.5** AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

	with an EAPOL LLC/Snap header. Allows for packet injection into an encrypted network.	
CVE-2020-26135	If a fragmented multi-destination packet is received, it will be accepted on encrypted networks if the fragment is plaintext. Allows for packet injection into an encrypted network.	**6.5** AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CVE-2020-26146	Encrypted fragments will be reassembled, even if they do not have consecutive packet numbers. When combined with fragment injection this can cause users to process malicious data.	**5.3** AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
CVE-2020-26147	Encrypted fragments will be reassembled, even if other fragments have been received plaintext. When combined with fragment injection this can cause users to process malicious data.	**5.4** AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:N

Symptoms

The CVEs discussed primarily create opportunities for packet injection attack vectors:

- Adversaries can inject/cause receipt of arbitrary TCP/IP packets that were never sent by the legitimate client or AP.
- Adversaries can exfiltrate data under specific conditions.
- Adversary can make the victim use the adversary's DNS server and intercept the victim’s traffic.
- Adversaries can get access to victim’s TCP ports that have active services listening (portscan).
- Adversaries may target delivery of illegitimate TCP/IP packets to any routable network devices.
- Adversary may route malicious traffic over operator network (hotspot mode).

Vulnerability Assessment

Affected Software

- All available versions of Wi-Fi AP software as per the impact matrix below

Affected Platforms

CVE ID	Access Points C-250 C-260 C-230 C-235 C-200	Access Points C-120 C-130 C-100 C-110 O-105 W-118	Access Points C-75 O-90 C-65 W-68
CVE-2020-24586	Y	N	N
CVE-2020-24587	Y	Y	Y
CVE-2020-24588	Y	Y	Y
CVE-2020-26139	Y	Y	N
CVE-2020-26140	N	N	Y
CVE-2020-26141	N	N	N
CVE-2020-26142	N	N	N
CVE-2020-26143	N	N	Y
CVE-2020-26144	Y	Y	Y
CVE-2020-26145	Y	Y	Y
CVE-2020-26146	Y	Y	Y
CVE-2020-26147	N	N	Y

Mitigation

As a security best practice, it is recommended to restrict public access to internal devices to safeguard from potential attacks. A machine-in-the-middle (MitM) attack is required to reliably exploit many of these vulnerabilities (except those applicable to the hotspot scenarios). In this type of attack the adversary sets up a clone of the real AP on a different channel and the client connects to this attacker’s clone instead of the real AP. This enables the attacker to block or modify 802.11 frames.

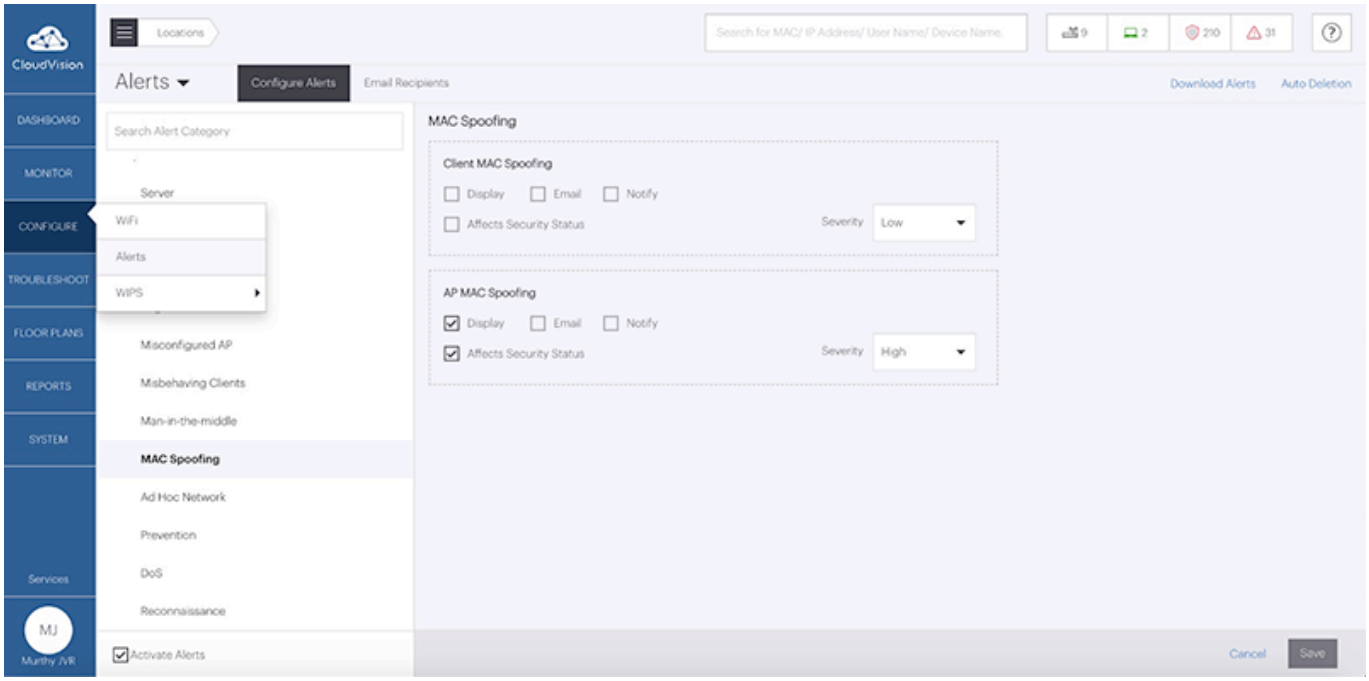
Arista Access Points are already capable of detecting Rogue APs spoofing the MAC address of a legitimate AP. They can also launch an automatic mitigation session in some cases to prevent legitimate clients from connecting to the Rogue AP. Arista AP models equipped with a dedicated scanning radio are capable of this detection and prevention features by scanning the entire spectrum.

Arista overlay WIPS solution can also detect and mitigate the Rogue AP spoofing attacks.

We recommend enabling the following WIPS settings if they are not already enabled:

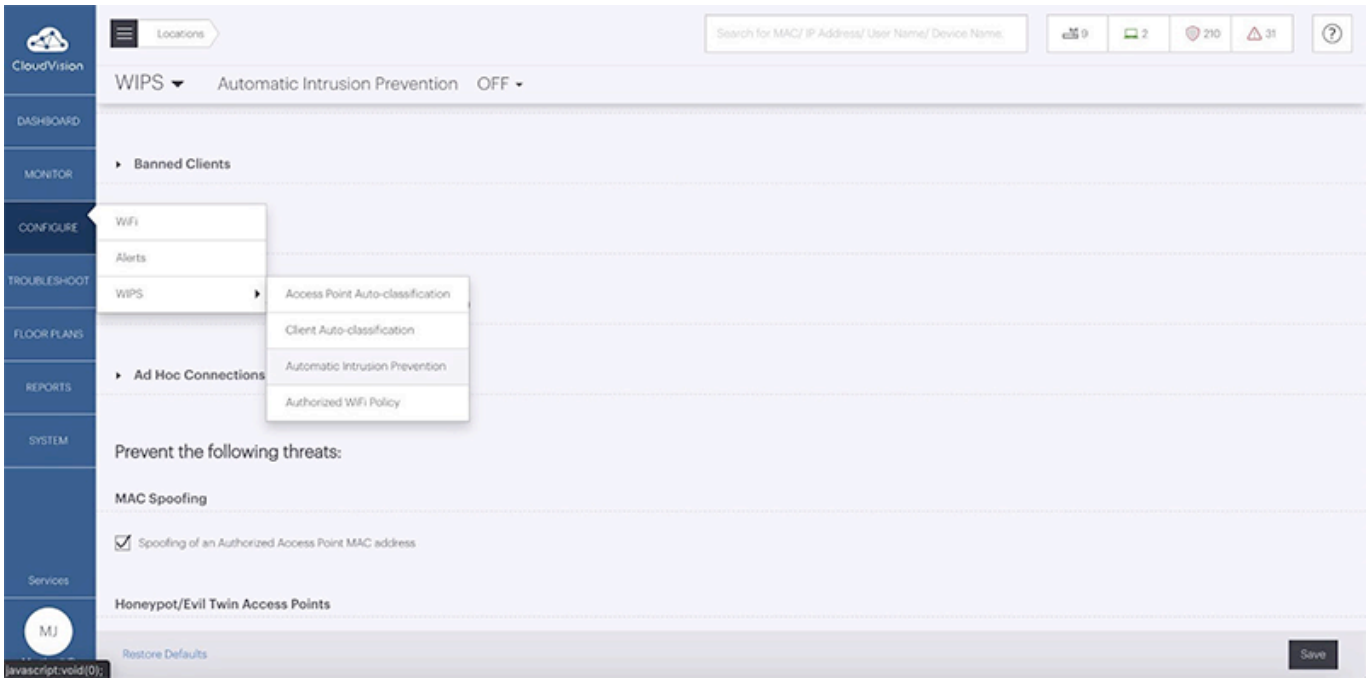
Configure > Alerts > MAC Spoofing > AP MAC Spoofing

Enable “Display” and “Affects Security Status”:



Configure > WIPS > Automatic Intrusion Detection > MAC Spoofing

Enable “Spoofing of an Authorized Access Point MAC address”:



As a full resolution against this vulnerability, refer to the next section for remediated software versions and hotfix details.

Resolution

This vulnerability is tracked by Bug 561363 and can manifest in any environment leveraging WEP, WPA, WPA2 and WPA3 security methods with any SSID for encryption. Arista is actively working with our chip vendors on incorporating fixes into Arista CloudVision Wi-Fi AP software. A new AP software version which addresses the above vulnerabilities will be released by Arista. This will be a regular upgrade similar to other new version upgrades. Arista will notify all customers and partners once the new version with the fixes is released and available. The recommended course of action is to install the provided hotfix or upgrade to a remediated CloudVision Wi-Fi AP software version once available.

Platform	Fixed Version	Release Date
C-260	**10.0.1-31**	**July 27, 2021**
C-250	**10.0.1-31**	**July 27, 2021**
C-230	**10.0.1-31**	**July 27, 2021**
C-200	**11.0.0-36**	**August 30, 2021**
C-130	**11.0.0-36**	**August 30, 2021**
C-120	**11.0.0-36**	**August 30, 2021**
C-110	**11.0.0-36**	**August 30, 2021**

C-100	**11.0.0-36**	**August 30, 2021**
C-75	*TBD*	*TBD*
C-65	*TBD*	*TBD*
O-235	**10.0.1-31**	**July 27, 2021**
O-105	**11.0.0-36**	**August 30, 2021**
O-90	*TBD*	*TBD*
W-118	**11.0.0-36**	**August 30, 2021**
W-68	*TBD*	*TBD*

Arista will notify all customers and partners as new versions with the fixes are released and available.

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

- On-prem deployments
- On-prem and Cloud deployments

For More Information

To read more about this vulnerability, please refer to the following links:

https://www.icasi.org/aggregation-fragmentation-attacks-against-wifi/

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-wifi@arista.com
By telephone: 408-547-5502 ; 866-476-0000