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 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.	**3.5** 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	**6.5** AV:A/AC:L/PR:N/UI:N/S:U/C:

	network if the frame begins with an EAPOL LLC/Snap header. Allows for packet injection into an encrypted network.	N/I:H/A:N
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