Hive Pro

THREAT ADVISORY

FragAttacks - Allowing adversaries to steal data by intercepting vulnerable network traffic from Wi-Fi devices	TA202111

Threat Level	Amber	Publish Date – May 17, 2021

Multiple vulnerabilities aka FragAttacks(**fr**agmentation and **ag**gregation **attacks**) have been found in Wi-Fi devices that makes most of the smartphones, servers, and operating systems susceptible to these. These vulnerabilities not only affect the latest Wi-Fi security protocol WPA3 but also affects the oldest protocol namely WEP which was released in 1997. Researchers have found 3 different types of flaws which includes Design Flaws(CVE-2020-24588, CVE-2020-24587, CVE-2020-24586), Implementation vulnerabilities that allow the trivial injection (CVE-2020-26145, CVE-2020-26144, CVE-2020-26140, CVE-2020-26143) and other implementation flaws (CVE-2020-26139,CVE-2020-26146,CVE-2020-26147,CVE-2020-26142,CVE-2020-26141)

Vulnerability Details

CVE ID	Vulnerability Name	Vulnerability Description	CWE ID
CVE-2020-24588	Accepting non-SPP A-MSDU frames, which leads to payload being parsed as an L2 frame under an A-MSDU bit toggling attack	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SPP A-MSDU frames, which is mandatory as part of 802.11n, an adversary can abuse this to inject arbitrary network packets.	
CVE-2020-24587	Reassembling fragments encrypted under different keys	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that all fragments of a frame are encrypted under the same key. An adversary can abuse this to exfiltrate selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP encryption key is periodically renewed.	CWE-200
CVE-2020-24586	Fragmentation cache not cleared on reconnection	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that received fragments must be cleared from memory after (re)connecting to a network. Under the right circumstances, when another device sends fragmented frames encrypted using WEP, CCMP, or GCMP, this can be abused to inject arbitrary network packets and/or exfiltrate user data.	CWE-74
CVE-2020-26145	Accepting plaintext broadcast fragments as full frames	Vulnerable WEP, WPA, WPA2, or WPA3 implementations accept second (or subsequent) broadcast fragments even when sent in plaintext and process them as full unfragmented frames. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.	CWE-74
CVE-2020-26144	Always accepting unencrypted A-MSDU frames that start with RFC1042 header with EAPOL ethertype	Vulnerable Wi-Fi implementations accept plaintext A-MSDU frames as long as the first 8 bytes correspond to a valid RFC1042 (i.e., LLC/SNAP) header for EAPOL. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.	

CVE ID	Vulnerability Name	Vulnerability Description	CWE ID
CVE-2020-26143	Accepting fragmented plaintext frames in protected networks	Vulnerable WEP, WPA, WPA2, or WPA3 implementations accept fragmented plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.	CWE-74
CVE-2020-26140	Accepting plaintext data frames in protected networks	Vulnerable WEP, WPA, WPA2, or WPA3 implementations accept plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.	CWE-74
CVE-2020-26139	Forwarding EAPOL from unauthenticated sender	Vulnerable Access Points (APs) forward EAPOL frames to other clients even though the sender has not yet successfully authenticated to the AP. An adversary might be able to abuse this in projected Wi-Fi networks to launch denial-of-service attacks against connected clients, and this makes it easier to exploit other vulnerabilities in connected clients.	CWE-404
CVE-2020-26146	Reassembling encrypted fragments with non-consecutive packet numbers	Vulnerable WPA, WPA2, or WPA3 implementations reassemble fragments with non-consecutive packet numbers. An adversary can abuse this to exfiltrate selected fragments. This vulnerability is exploitable when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used. Note that WEP is vulnerable to this attack by design.	CWE-74
CVE-2020-26147	Reassembling mixed encrypted/plaintext fragments	Vulnerable WEP, WPA, WPA2, or WPA3 implementations reassemble fragments even though some of them were sent in plaintext. This vulnerability can be abused to inject packets and/or exfiltrate selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used.	CWE-74
CVE-2020-26142	Processing fragmented frames as full frames	Vulnerable WEP, WPA, WPA2, or WPA3 implementations treat fragmented frames as full frames. An adversary can abuse this to inject arbitrary network packets, independent of the network configuration.	CWE-74
CVE-2020-26141	Not verifying TKIP MIC of fragmented frames	Vulnerable Wi-Fi implementations do not verify the Message Integrity Check (authenticity) of fragmented TKIP frames. An adversary can abuse this to inject and possibly decrypt packets in WPA or WPA2 networks that support the TKIP data-confidentiality protocol.	CWE-924

Patch Link

https://github.com/vanhoefm/fragattacks/blob/master/ADVISORIES.md

References

https://github.com/vanhoefm/fragattacks
https://www.fragattacks.com/
https://www.openwall.com/lists/oss-security/2021/05/11/12
https://latesthackingnews.com/2021/05/16/fragattacks-newly-discovered-vulnerabilities-affect-wifi-and-iot-devices/