dSA210511
Fragment and Forge vulnerabilities: Breaking Wi-Fi Through Frame Aggregation and Fragmentation

Published: 2021-05-12
Last updated: (initial version)
Document version: 1.0

Notice

devolo AG is aware of multiple security vulnerabilities in Wi-Fi components used in devolo products. Exploitation of these vulnerabilities could cause denial of service, injection of arbitrary network packets or exfiltration of user data.

The information in this document is subject to change without notice and should not be construed as a commitment by devolo AG. All information that relates to the future (e.g., planned software versions and release dates) is provided without guarantee.

Affected Product and Version

All devolo devices offering Wi-Fi
version 5.8.0 and earlier

Vulnerability Details

CVE-2020-24586

CWE ID: CWE-310

Description: Some devices may not clear received fragments 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.

CVE-2020-24587

CWE ID: CWE-310

Description: Some devices do not require that all fragments of a frame are encrypted under the same key. An adversary can abuse this to exfiltrate selected fragments when an adversary device sends fragmented frames and the encryption key is renewed. Encryption keys are renewed periodically under scenarios such as a session key renewal or roaming to a new access point.

CVE-2020-24588

CWE ID: CWE-287

Description: The IEEE 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) defines two variants of A-MSDU protection where the commonly deployed one does not protect the A-MSDU Present subfield in the plaintext QoS header field. An adversary can abuse this to inject arbitrary network packets when this variant is enabled.

CVE-2020-26139

CWE ID: CWE-287

Description: 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 protected Wi-Fi networks to launch denial-of-service attacks against connected clients, and this makes it easier to exploit other vulnerabilities in connected clients.

CVE-2020-26140

CWE ID: CWE-287

Description: 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.

CVE-2020-26141

CWE ID: CWE-310

Description: 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.

CVE-2020-26142

Not affected.

CVE-2020-26143

CWE ID: CWE-287

Description: 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.

CVE-2020-26144

CWE ID: CWE-287

Description: Vulnerable implementations accept all subframes except the first subframe of plaintext AMSDU frames as long as the first 6 to 8 bytes correspond to a valid RFC1042 (i.e., EAPOL LLC/SNAP) header for EAPOL. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.

CVE-2020-26145

CWE ID: CWE-287

Description: 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.

CVE-2020-26146

CWE ID: CWE-310

Description: Vulnerable WPA, WPA2, or WPA3 implementations reassemble fragments with nonconsecutive 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.

CVE-2020-26147

CWE ID: CWE-310

Description: 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.

CVE-2020-11264

CWE ID: CWE-287

Description: Vulnerable Access Points (APs) may accept and process plaintext unicast Wi-Fi frames while authentication to an encrypted network is occurring allowing an adversary to inject arbitrary network packets independent of the network configuration.

CVE-2020-11301

CWE ID: CWE-287

Description: Vulnerable Access Points (APs) may accept and process broadcast packets before, during and after authentication to an encrypted network allowing an adversary to inject arbitrary network packets independent of the network configuration.

Remediation and Mitigation

Customers are advised to update to the upcoming firmware version 5.8.1 upon availability.

Customers are generally advised to take appropriate measures to protect access to the WLAN that the device is operated in. Other devices connected to the Wi-Fi network should be updated with the latest firmware that fixes these vulnerabilities. To mitigate attacks that steal user information, double-check that HTTPS is used for connections, e.g. to websites. For sensitive networks, as mitigation the Wi-Fi can be turned off until the firmware update has been installed in all devices.

Acknowlegements

devolo AG thanks the following parties for their efforts:
* Qualcomm Technologies
* Mathy Vanhoef, New York University Abu Dhabi