Message-ID: <ae9de74624a11f32da8edd8c195b753c7d177d3b.camel@sipsolutions.net>
Date: Tue, 11 May 2021 20:11:03 +0200
From: Johannes Berg <johannes@...solutions.net>
To: oss-security@...ts.openwall.com
Cc: Jouni Malinen <j@...fi>
Subject: various 802.11 security issues - fragattacks.com

Hi,

Several security issues in the 802.11 implementations were found by
Mathy Vanhoef (New York University Abu Dhabi), who has published all
the details at

https://papers.mathyvanhoef.com/usenix2021.pdf

and

https://www.fragattacks.com/

For Linux, we've developed the set of patches posted here:

https://lore.kernel.org/linux-wireless/20210511180259.159598-1-johannes@sipsolutions.net/

Specifically, the following CVEs were assigned:

 * CVE-2020-24586 - Fragmentation cache not cleared on reconnection
 * CVE-2020-24587 - Reassembling fragments encrypted under different
                    keys
 * 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
 * CVE-2020-26139 - Forwarding EAPOL from unauthenticated sender
 * CVE-2020-26140 - Accepting plaintext data frames in protected
                    networks
 * CVE-2020-26141 - Not verifying TKIP MIC of fragmented frames
 * CVE-2020-26142 - Processing fragmented frames as full frames
 * CVE-2020-26143 - Accepting fragmented plaintext frames in
                    protected networks
 * CVE-2020-26144 - Always accepting unencrypted A-MSDU frames that
                    start with RFC1042 header with EAPOL ethertype
 * CVE-2020-26145 - Accepting plaintext broadcast fragments as full
                    frames
 * CVE-2020-26146 - Reassembling encrypted fragments with non-consecutive
                    packet numbers
 * CVE-2020-26147 - Reassembling mixed encrypted/plaintext fragments

In general, the scope of these attacks is that they may allow an
attacker to
 * inject L2 frames that they can more or less control (depending on the
   vulnerability and attack method) into an otherwise protected network;
 * exfiltrate (some) network data under certain conditions, this is
   specific to the fragmentation issues.

A subset of these issues is known to apply to the Linux IEEE 802.11
implementation (mac80211). Where it is affected, the attached patches
fix the issues, even if not all of them reference the exact CVE IDs.

In addition, driver and/or firmware updates may be necessary, as well
as potentially more fixes to mac80211, depending on how drivers are
using it.

```
Specifically, for Intel devices, firmware needs to be updated to the
most recently released versions (which was done without any reference
to the security issues) to address some of the vulnerabilities.

To have a single set of patches, I have included the patches for ath10k
and ath11k drivers in my patch posting linked to above.

We currently don't have information about how other drivers are, if
at all, affected.

Thanks,
johannes
```