WESTERMO-21-02: Security Advisory

CRITICAL / HIGH / **MEDIUM** / LOW / INFORMATIONAL 2021-07-19

Security Vulnerability in the wireless 802.11 implementation

List of CVEs

- 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

Description

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

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.

The fragmentation and mixed key vulnerabilities need Man-In-The-Middle type of attack where one sets a forwarding AP/STA between the victim and legit AP. An attacker has to be connected to the victim, so it has to first setup it to match victim security credentials which in theory limits this to public/open wifi cases. Then the victim has to be forced to connect to this AP which would imply close physical vicinity.

Once attacker controls connection he/she can inject frames which support other type of the attack like ARP/DNS poisoning or using mixed keys to leak information about secrets in cipher.

Affected versions

All Ibex products running SW6 firmware version 6.9.5 RC1 and older

Severity

The CVSSv3 severity base score for the CVEs is:

CVE-2020-24586: **2.9**
CVE-2020-24587: **1.8**
CVE-2020-24588: **2.9**
CVE-2020-26139: **2.9**
CVE-2020-26140: **3.3**
CVE-2020-26141: **3.3**
CVE-2020-26142: **5.0**
CVE-2020-26143: **3.3**
CVE-2020-26144: **3.3**
CVE-2020-26145: **3.3**
CVE-2020-26146: **2.9**
CVE-2020-26147: **3.2**

Mitigation

- Disable any activated wireless functionality in your Ibex product
- Update to the latest firmware available for your product. All versions **6.9.5 RC2 or newer** are no longer vulnerable to the above CVEs.

References

https://www.fragattacks.com/
Download Ibex series v.6.9.5 (zip, 45 MB)