Overview

Multiple Vulnerabilities in Treck IP Stack - VU#257161.

Several previously unknown vulnerabilities in the Treck TCP/IP stack implementation have been discovered by an independent security research company JSOF. The vulnerabilities are collectively referred to the nickname “Ripple20” and listed as Vulnerability Note VU#257161. The main vulnerability affecting Intesis Wireless devices is the CVE-2020-11901.

This third party closed source library that provides TCP/IP network services, is used in several legacy wireless Intesis products.

Impact

Successful exploitation of this vulnerability may allow a remote attacker to perform remote code execution.

Affected products and versions

IntesisHome/AC cloud products. They are connected outside the local network and are quite exposed to the exploitation of the vulnerability. The following products with Config FW version ≤ 2.0.17 and Runtime FW version ≤ 2.0.40 are affected:

- DK-AC-WIFI-1A
- DK-RC-WIFI-1
- FJ-IR-WIFI-1NA
- FJ-RC-WIFI-1
- FJ-RC-WIFI-1NA
- IS-IR-WIFI-1
- IS-IR-WIFI-1NA
- LG-RC-WIFI-1
- MH-RC-WIFI-1
- OAE-TO-RC-WIFI-1
- OIM-IS-IR-WIFI-1
- OLE-LG-AW-WF-1
- OLE-LG-IR-WF-1
- OPE-PAW-IR-WIFI-1
- PA-AC-WIFI-1
- PA-AC-WIFI-1A
- PA-AC-WIFI-1L
• PA-AW-WIFI-1
• PA-AW-WIFI-1TE
• PA-RC2-WIFI-1
• TO-RC-WIFI-1

Wifi AC interfaces. They are typically working only on a local network so it would be quite hard that someone would exploit the vulnerability. The following products with Config FW version ≤ 1.0.2 and Runtime FW version ≤ 1.0.7 are affected:

• DK-AC-WMP-1
• DK-RC-WMP-1
• FJ-RC-WMP-1
• IS-IR-WMP-1
• IBWMUPI001I023
• LG-RC-WMP-1
• ME-AC-WMP-1
• MH-RC-WMP-1
• PA-AC-WMP-1
• PA-RC2-WMP-1
• TO-RC-WMP-1

Severity / CVSS Score

The following CVE have been fixed in the products.

<table>
<thead>
<tr>
<th>CVE ID</th>
<th>CVSS 3.1 Rating</th>
<th>CVSS 3.1 Vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2020-11904</td>
<td>5,6</td>
<td>CVSS:3.1/AV:N/AC:H /PR:N/UI:N/S:U/C:L/I:L/A:L</td>
</tr>
</tbody>
</table>

Product updates

Updates with all the fixes are currently available and released.

IntesisHome/AC cloud products connected devices have been automatically updated with Config FW version ≥ 2.0.18 and Runtime FW version ≥ 2.0.41. The ones disconnected will also automatically update once they connect to the server.

Wifi AC interfaces require a manual action using the configuration software in order to update to Config FW version ≥ 1.0.3 and Runtime FW version ≥ 1.0.8.

---

1 CVSS is owned by FIRST and used by permission. https://www.first.org/cvss

HMS Industrial Networks AB, PO Box 4126, 300 04 Halmstad, Sweden
Tel. +46 35 17 29 00, www.hms-networks.com
HMS Recommendations

HMS recommends updating all the Wifi AC interfaces installed in the field. If both the local network and DNS server are considered to be secure this would not be required.

IntesisHome/AC cloud products do not require any action as they are automatically updated.