Overview

Multiple Vulnerabilities in Treck IP Stack - VU#257161

This third party closed source library that provides TCP/IP network services, also known as the Treck TCP/IP network stack, is used in several HMS products.

Several previously unknown vulnerabilities in the Treck TCP/IP stack implementation have been discovered by the independent security research company JSOF. The vulnerabilities are known under the collective name “Ripple20” and are listed as Vulnerability Note VU#257161

Impact

If your device is not using any TCP/IP communication (Ethernet interface) your product is not affected.

If your device is installed on a network then it may be possible, under specific circumstances, that these vulnerabilities could lead to a remote code execution via a network-based attack without authentication, or denial of service (DoS), or information disclosure.

If your device is installed on a local network, the risk is significantly lower as presumptive attackers need access to the local network to do harm.

Affected EOL Products

HMS LABSline SG

- LABSG10W104  SG-10 with I/O and IEC 60870-5-104
- LABSG10W850  SG-10 with I/O and IEC 61850
- LABSG10W954  SG-10 with I/O and IEC 61850 + IEC 60870-5-104
- LABSG11W104  SG-11 with M-Bus master and IEC 60870-5-104
- LABSG11W850  SG-11 with M-Bus master and IEC 61850
- LABSG11W954  SG-11 with M-Bus master and IEC 61850 + IEC 60870-5-104
- LABSG40W104  SG-40 with PROFINET and IEC 60870-5-104
- LABSG40W850  SG-40 with PROFINET and IEC 61850
- LABSG40W954  SG-40 with PROFINET and IEC 60870-5-104

Anybus SG-gateways

- ASG10??-B  Anybus SG-gateway with I/O
- ASG11??-B  Anybus SG-gateway with M-Bus Master
- ASG40??-B  Anybus SG-gateway with PROFINET
- ASG41??-B  Anybus SG-gateway with EtherNet/IP
- ASG42??-B  Anybus SG-gateway with PROFIBUS

NOTE: ?? = any item code variation (codes from 00 to 15)

NOTE: Ixxat SG-gateways (Item codes ASG-????-C, ISG-????-C) are not affected!
CVE Entry / CVSS Score

The following CVEs with a CVSS\(^1\) severity base score ≥ 5 are currently determined:

<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-2020-11898</td>
<td>9,1</td>
<td>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U:C:H/I:N/A:H</td>
</tr>
<tr>
<td>CVE-2020-11900</td>
<td>8,2</td>
<td>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U:C:N/I:L/A:H</td>
</tr>
</tbody>
</table>

HMS Recommendations

As the above listed products are EOL and therefore not maintained anymore, HMS recommends that the products are replaced by Ixxat SG-gateways (order codes ASG-????-C, ISG-????-C) which are not affected by this vulnerability and are under continuous maintenance.

In cases where the product cannot be replaced, HMS recommends disconnecting the product from the network or implementing extra security controls. In addition to general recommendations such as using a properly configured firewall, vulnerability specific recommendations can be found at this weblink: https://github.com/CERTCC/PoC-Exploits/blob/master/vu-257161/recommendations.md

Additional Information

For questions and support regarding this or any other product issues please contact us via https://mysupport.hms.se

---

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