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/Beck products and is a part of the Operating System RTOS@CHIP.

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.

Impact

If your device is not using any TCP/IP communication (Ethernet interface) your products 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 products and versions

IPC@CHIP Family SC2x, SC1x3 with RTOS ≤ V2.05

- 543258  IPC@CHIP SC143-LF
- 543260  IPC@CHIP SC143-IEC-LF
- 570582  IPC@CHIP SC143-PIS-LF
- 570744  IPC@CHIP SC143-LF-IEC-PIS
- 566821  IPC@CHIP SC24
- 566822  IPC@CHIP SC24-IEC
- 570592  IPC@CHIP SC24-PIS
- 570682  IPC@CHIP SC24-IEC-PIS
- 570700  IPC@CHIP SC24-ETR
- 570705  IPC@CHIP SC24-IEC-ETR
- 570830  IPC@CHIP SC24-IEC-PIS-ETR

IPC@CHIP Family SC243 with RTOS-PPC ≤ V1.80

- 563963  IPC@CHIP SC243
- 570736  IPC@CHIP SC243-IEC3
Affected discontinued Products

IPC@CHIP Family SC2x, SC1x3 with RTOS ≤ V2.05

- 543257  IPC@CHIP SC123-LF
- 543259  IPC@CHIP SC123-IEC-LF
- 553944  IPC@CHIP SC23
- 553945  IPC@CHIP SC23-IEC

CVE Entry / CVSS Score

The following CVEs 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: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:C:N/I:L/A:H</td>
</tr>
<tr>
<td>CVE-2020-11902</td>
<td>7.3</td>
<td>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C:L/I:L/A:L</td>
</tr>
<tr>
<td>CVE-2020-11903</td>
<td>5.3</td>
<td>CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C:H/I:N/A:N</td>
</tr>
<tr>
<td>CVE-2020-11909</td>
<td>3.7</td>
<td>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C:L/I:N/A:N</td>
</tr>
<tr>
<td>CVE-2020-11910</td>
<td>3.7</td>
<td>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C:L/I:N/A:N</td>
</tr>
<tr>
<td>CVE-2020-11911</td>
<td>3.7</td>
<td>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C:N/I:N/A:L</td>
</tr>
<tr>
<td>CVE-2020-11912</td>
<td>3.7</td>
<td>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C:L/I:N/A:N</td>
</tr>
<tr>
<td>CVE-2020-11913</td>
<td>3.7</td>
<td>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C:L/I:N/A:N</td>
</tr>
<tr>
<td>CVE-2020-11908</td>
<td>3.1</td>
<td>CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C:N/I:N/A:L</td>
</tr>
<tr>
<td>CVE-2020-11914</td>
<td>3.1</td>
<td>CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C:L/I:N/A:N</td>
</tr>
</tbody>
</table>

HMS Recommendations

HMS recommends that the products are updated to the latest RTOS@CHIP Version (RTOS-PPC V1.90, RTOS V 2.06) where the issues has been fixed.

In cases where the product cannot be updated, HMS recommends disconnecting the product from 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.

---

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

Updates are available here:

IPC@CHIP Family SC2x, SC1x3: [https://www.beck-ipc.com/en/produkte/rtos/](https://www.beck-ipc.com/en/produkte/rtos/)


Additional information

For questions and support regards this or any other product issues please contact us at support@beck-ipc.com.

Affected EOL Products

The following table lists the affected EOL products which are already no longer supplied and no longer maintained.

IPC@CHIP Family SC1x with all RTOS Versions.

- 20040112  IPC@CHIP SC12
- 537227  IPC@CHIP SC12-F
- 542490  IPC@CHIP SC12-LF
- 552379  IPC@CHIP SC12B-LF
- 552380  IPC@CHIP SC12B-F-LF
- 536079  IPC@CHIP SC13
- 538429  IPC@CHIP SC13-F
- 540553  IPC@CHIP SC13-IEC
- 542546  IPC@CHIP SC13-LF
- 542547  IPC@CHIP SC13-F-LF
- 542752  IPC@CHIP SC13-IEC-LF

BC Compact WEB Controller with all RTOS Versions.

- 20020231  WEB Controller BC440
- 537037  WEB Controller BC452
- 537038  WEB Controller BC454
- 20020264  WEB Controller BC660
## CVE Entry / CVSS Score

The following CVEs are currently determined:

<table>
<thead>
<tr>
<th>CVE ID</th>
<th>CVSS 3.1 Rating</th>
<th>CVSS 3.1 Base Vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2020-11909</td>
<td>3,7</td>
<td>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N</td>
</tr>
<tr>
<td>CVE-2020-11911</td>
<td>3,7</td>
<td>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L</td>
</tr>
<tr>
<td>CVE-2020-11912</td>
<td>3,7</td>
<td>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N</td>
</tr>
<tr>
<td>CVE-2020-11908</td>
<td>3,1</td>
<td>CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L</td>
</tr>
</tbody>
</table>

---

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