HMS Security Advisory Report

HMSSAR-2021-01-04-001

Publication date: 04 January 2021
Last update: 04 January 2021

Overview

Some Vulnerabilities in Treck IP Stack - VU#114986

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.

Impact

If your device is not using any TCP/IP communication your products is not affected.

If your device is not using the Webserver your product is not affected with CVE-2020-25066.

If your device is not using IPv6 your product is not affected with CVE-2020-27336 and CVE-2020-27337.

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 ≤ V2.06

- 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 ≤ V1.90

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

IPC@CHIP Family SC2x, SC1x3 with RTOS ≤ V2.06

- 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-2020-27336</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-2020-27337</td>
<td>7,3</td>
<td>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L</td>
</tr>
</tbody>
</table>

**HMS Recommendations**

HMS recommends that the products are updated to the latest RTOS@CHIP Version (RTOS-PPC V1.91, RTOS V 2.07) 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](https://github.com/CERTCC/PoC-Exploits/blob/master/vu-257161/recommendations.md).

**Product updates**

Updates are available here:


**Additional information**

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

---

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