Health Sector Cybersecurity Coordination Center (HC3)

**Analyst Note**

**January 4, 2021** **TLP: White** **Report: 202101040830**

# TCP/IP Stack Vulnerabilities Possibly Affect Healthcare Devices

## Executive Summary

On December 8, 2020, a report titled Amnesia:33 developed by Forescout disclosed multiple zero-day vulnerabilities in the TCP/IP stacks impacting numerous Operational Technology (OT), Internet of Things (IoT), Building Automation Systems, and Information Technology (IT) devices. The 33 vulnerabilities could cause denial of service, unauthorized information disclosure and several remote code execution errors. According to Forescout, at least 150 vendors may have implemented libraries affected by Amnesia:33. Of the 33 reported vulnerabilities, 3 were classified as critical and require immediate attention.

## Report

Following the Amnesia 33 report by Forescout which identified 33 vulnerabilities CISA released a separate ICS Advisory (ICSA-20-343-01) which provided additional details and mitigation activities.

The specific TCP/IP stacks affected include:

- uIP (end-of-life [EOL]) versions 1.0 and prior
- uIP-Contiki-OS [EOL] versions 3.0 and prior
- uIP-Contiki-NG versions 4.6.0 and prior
- *open-iscsi versions 2.1.12 and prior
- picoTCP-NG versions 1.7.0 and prior
- picoTCP (EOL) versions 1.7.0 and prior
- FNET versions 4.7.0 and prior
- Nut/Net versions 5.1 and prior
- *Treck versions 6.0.1.67 and prior

*open-iscsi (small computer system interface) services insert a variant of the affected uIP stack and are affected by a small portion of the CVEs mentioned in CVE table below. The Treck TCP/IP stack may be known by other names such as Kasago TCP/IP, ELMIC, Net+ OS, Quadnet, GHNET v2, Kwiknet, or AMX.

The disclosed TCP/IP stacks serves as essential communication protocols for millions of OT, IoT, Building Automation Systems, and IT devices. The affected stacks have the potential to cause the following vulnerabilities:

| Vulnerability | Example Exploit |
|---|---|
| **Infinite Loop** | function used to process IPv6 extension headers and extension header options can be forced into an infinite loop state due to unchecked header/option lengths. |
| **Integer Wraparound** | function used to decapsulate RPL extension headers does not check for unsafe integer conversion when parsing the values provided in a header, allowing an attacker to corrupt memory. |
| **Integer Overflow** | function that parses the TCP MSS option does not check the validity of the length field of this option, allowing an attacker to force it into an infinite loop when arbitrary TCP MSS values are supplied. |

| Vulnerability | Example Exploit |
|---|---|
| Out-of bounds Read | function that parses incoming transport layer packets (TCP/UDP) does not check the length fields of packet headers against the data available in the packets. Given arbitrary lengths, an out-of-bounds memory read may be performed during the checksum computation. |
| Out-of- bounds Write | When handling TCP urgent data, there are no sanity checks for the value of the urgent data pointer, allowing an attacker to corrupt memory by supplying arbitrary urgent data pointer offsets within TCP packets. |
| Improper Null Termination | When parsing incoming DNS packets, there are no checks whether domain names are null terminated. This allows an attacker to achieve memory corruption with crafted DNS responses. |
| Improper Input Validation- | the payload length field of IPv6 extension headers are not checked against the data available in incoming packets, allowing an attacker to corrupt memory. |
| Heap-Based Buffer Overflow | A vulnerability in Treck HTTP Server components allow an attacker to cause a denial-of-service condition. This vulnerability may also result in arbitrary code execution. |

## Analyst Comment:

The rise of the use of IOT devices in the healthcare environment makes these vulnerabilities particularly important for the healthcare and public (HPH) Sector. Once an attacker uses these vulnerabilities to get into the entities environment they can then cause an unknown number of issues. IOT devices are also often difficult to update and therefore remain unpatched, making them a well known and easy entry point for threat actors. A non-segmented network the attacker was able to access several devices disrupting their normal functions.  Additionally, maintaining updates for TCP/IP stacks can assist with eliminating the possibility of a remote code execution, denial of service, and unauthorized information disclosure.

## Patches, Mitigations & Workarounds:

### Mitigations

If an organization has adopted this software from an external entity, it’s recommended that the organization contact the provider to get appropriate updates for integrated stacks within software. Once validated by the organization, update to the latest patches for specified TCP/IP stacks.

Additional recommendations:

- Ensure default passwords are changed and secured.
- Disable unused features and services on your embedded devices.
- Avoid exposure of IoT and embedded devices directly over the Internet and use a segmented network zone when available.
- Enable security features such as deep-packet inspection and firewall anomaly detection when available to protect embedded and IoT devices.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available.

**Patches**

Further details, including any available patches, will be included in the corresponding CVE entries below:

Amnesia:33

| CVE | Affected Stack | Vulnerability Type | Impact | CVSSv3 |
|---|---|---|---|---|
| CVE-2020-13984 | uIP | Infinite Loop | Denial of Service | 7.5 |
| CVE-2020-13985 | uIP | Integer Wraparound | Denial of Service | 7.5 |
| CVE-2020-13986 | uIP | Integer Loop | Denial of Service | 7.5 |
| CVE-2020-13987 | uIP<br>open-iscsi | Out-of-Bounds Read | Denial of Service, Information Leak | 8.2 |
| CVE-2020-13988 | uIP<br>open-iscsi | Integer Overflow | Denial of Service | 7.5 |
| CVE-2020-17437 | uIP<br>open-iscsi | Out-of-Bounds Write | Denial of Service | 8.2 |
| CVE-2020-17438 | uIP<br>open-iscsi | Out-of-Bounds Write | Denial of Service | 7 |
| CVE-2020-17439 | uIP | Improper Input Validation | DNS Cache Poisoning | 8.1 |
| CVE-2020-17440 | uIP | Improper Input Validation | Denial of Service | 7.5 |
| CVE-2020-24334 | uIP | Out-of-Bounds Read | Denial of Service | 8.2 |
| CVE-2020-24335 | uIP | Out-of-Bounds Read | Denial of Service | 7.5 |
| CVE-2020-24336 | uIP | Out-of-Bounds Read | Remote Code Execution | 9.8 |
| CVE-2020-25112 | uIP | Out-of-Bounds Write | Remote Code Execution | 8.1 |
| CVE-2020-17441 | picoTCP | Improper Input Valiation | Denial of Service, Information Leak | 7.5 |
| CVE-2020-17442 | picoTCP | Integer Overflow | Denial of Service | 7.5 |
| CVE-2020-17443 | picoTCP | Integer Overflow | Denial of Service | 8.2 |
| CVE-2020-17444 | picoTCP | Out-of-Bounds Read | Denial of Service | 7.5 |
| CVE-2020-17445 | picoTCP | Out-of-Bounds Read | Denial of Service | 7.5 |
| CVE-2020-24337 | picoTCP | Infinite Loop | Denial of Service | 7.5 |
| CVE-2020-24338 | picoTCP | Out-of-Bounds Write | Remote Code Execution | 9.8 |
| CVE-2020-24339 | picoTCP | Out-of-Bounds Read | Denial of Service | 7.5 |
| CVE-2020-24340 | picoTCP | Out-of-Bounds Read | Denial of Service, Information Leak | 8.2 |
| CVE-2020-24341 | picoTCP | Out-of-Bounds Read | Denial of Service, Information Leak | 8.2 |
| CVE-2020-17467 | FNET | Out-of-Bounds Read | Information Leak | 8.2 |
| CVE-2020-17468 | FNET | Out-of-Bounds Read | Denial of Service | 7.5 |
| CVE-2020-17469 | FNET | Out-of-Bounds Read | Denial of Service | 5.9 |
| CVE-2020-17470 | FNET | Improper Input Validation | DNS Cache Poisoning | 4 |
| CVE-2020-24383 | FNET | Improper Null Termination | Denial of Service, Information Leak | 6.5 |
| CVE-2020-25107 | Nut/Net | Out-of-Bounds Read | Denial of Service | 7.5 |
| CVE-2020-25108 | Nut/Net | Out-of-Bounds Write | Denial of Service | 7.5 |
| CVE-2020-25109 | Nut/Net | Out-of-Bounds Read | Denial of Service | 8.2 |
| CVE-2020-25110 | Nut/Net | Out-of-Bounds Read | Denial of Service | 8.2 |
| CVE-2020-25111 | Nut/Net | Out-of-Bounds Write | Remote Code Execution | 9.8 |

ICSA-20-353-01 (Treck)

| CVE | Affected Stack | Vulnerability Type | Impact | CVSSv3 |
|---|---|---|---|---|
| CVE-2020-25066 | Treck | Heap-Based Buffer Overflow | Denial of Service | 9.3 |
| CVE-2020-27336 | Treck | Out-of-Bounds Read | Remote Code Execution | 3.7 |
| CVE-2020-27337 | Treck | Out-Of-Bounds Write | Remote Code Execution, Denial of Service | 9.1 |
| CVE-2020-27338 | Treck | Out-of-Bounds Read | Remote Code Execution, Denial of Service | 5.9 |

## References

Amnesia:33 Identify and Mitigate the Risk From Vulnerabilities Lurking in Millions of IoT, OT and IT Devices
https://www.forescout.com/company/resources/amnesia33-identify-and-mitigate-the-risk-from-vulnerabilities-lurking-in-millions-of-iot-ot-and-it-devices/

AMNESIA:33: Researchers Disclose 33 Vulnerabilities Across Four Open Source TCP/IP Libraries
https://www.tenable.com/blog/amnesia33-researchers-disclose-33-vulnerabilities-tcpip-libraries-uip-fnet-picotcp-nutnet

ICS Advisory (ICSA-20-343-01)
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-01

Embedded TCP/IP stacks have memory corruption vulnerabilities
https://www.kb.cert.org/vuls/id/815128

Third-party libraries are one of the most insecure parts of an application
https://techbeacon.com/security/third-party-libraries-are-one-most-insecure-parts-application

SUSE statement on Amnesia:33 vulnerabilities
https://www.suse.com/c/suse-statement-on-amnesia33-vulnerabilities/

PicoTCP User Documentation
https://os.mbed.com/media/uploads/daniele/user_doc.pdf

Embedded TCP/IP stacks have memory corruption vulnerabilities
https://www.kb.cert.org/vuls/id/815128

ICS Advisory (ICSA-20-353-01)
https://us-cert.cisa.gov/ics/advisories/icsa-20-353-01

CISA Issues ICS Advisory for New Vulnerabilities in Treck TCP/IP Stack
https://www.securityweek.com/cisa-issues-ics-advisory-new-vulnerabilities-treck-tcpip-stack