Application Report

Amnesia Open-Source TCP/IP Stack Vulnerabilities (AMNESIA:33)

TI-PSIRT-2020-100078

Publication date: December 21, 2020

Summary

Forescout Research Labs has identified potential vulnerabilities in multiple open-source TCP/IP stacks. The following potential vulnerabilities have been identified as impacting the uIP and Contiki-OS software:

CVEID	CVSS Score	CVSS Vector	Description
CVE-2020-13985	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	The function used to decapsulate RPL extension headers does not check for unsafe integer conversion when parsing the values provided in a header, allowing attackers to corrupt memory.
CVE-2020-13984	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	The function used to process IPv6 extension headers and extension header options can be put into an infinite loop state due to unchecked header/option lengths.
CVE-2020-13986	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	The function used to decapsulate RPL extension headers does not check the length value of an RPL extension header received, allowing attackers to put it into an infinite loop.
CVE-2020-13988	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	The function that parses the TCP MSS option does not check the validity of the length field of this option, allowing attackers to put it into an infinite loop, when arbitrary TCP MSS values are supplied.
CVE-2020-17440	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	When parsing incoming DNS packets, there are no checks whether domain names are null-terminated. This allows attackers to achieve memory corruption with crafted DNS responses.
CVE-2020-24335	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	The function that parses domain names lacks bounds checks, allowing attackers to corrupt memory with crafted DNS packets.
CVE-2020-13987	8.2	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	The 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.
CVE-2020-24334	8.2	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	The code that processes DNS responses does not check whether the number of responses specified in the DNS packet header correspond to the response data available in the DNS packet, allowing attackers to corrupt memory.
CVE-2020-17437	8.2	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	When handling TCP Urgent data, there are no sanity checks for the value of the Urgent data pointer, allowing attackers to corrupt memory by supplying arbitrary Urgent data pointer offsets within TCP packets.
CVE-2020-24336	9.8	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	The code for parsing DNS records in DNS response packets sent over NAT64 does not validate the length field of the response records, allowing attackers to corrupt memory.
CVE-2020-25112	8.1	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	Several issues, such as insufficient checks for the IPv4/IPv6 header length and inconsistent checks for the IPv6 header extension lengths, allow attackers to corrupt memory.

Affected products and versions

Legacy Texas Instruments example software for 6LoWPAN solutions is likely impacted.

It is also possible that the CVE-2020-13986 potential vulnerability affects the uIP version shipped in the MSP432E4 SDK example project boot_serial_emac_flash_MSP_EXP432E401Y_nortos. As shipped, the example code in the project is not directly vulnerable because UDP checksums are not enabled (UIP_CONF_UDP_CHECKSUMS is not defined in uip-conf.h). However, it is a best practice to enable UDP checksums during deployment.

Potentially impacted features

The example TI reference designs for 6LoWPAN networks listed below were provided on TI.com and contained example software for implementing 6LoWPAN networks based on the Contiki-OS RTOS. This example implementation included the uIP TCP/IP stack, identified to be potentially vulnerable.

- https://www.ti.com/tool/TIDA-010003
- https://www.ti.com/tool/TIDA-010024
- https://www.ti.com/tool/TIDA-010032

Suggested mitigations

Due to the legacy nature of the example software, the above TI reference designs for 6LoWPAN networks are considered obsolete, and as such there is no plan to update them at this time. It is recommended that TI customers who referenced example software that included Contiki-OS evaluate the recommendations provided by the ICS Advisory and either:

1. Ensure they take appropriate actions to mitigate these potential vulnerabilities in Contiki-OS, or
2. Move to Contiki-NG 4.6.

It is recommended that customers who have used MSP432E4 SDK example project boot_serial_emac_flash_MSP_EXP432E401Y_nortos and enabled UDP checksums upgrade their uIP handling to a version of Contiki's uIP software stack above version 3.0.

External references

- Forescout AMNESIA:33 public report
- ICS Advisory (ICSA-20-343-01)
- Contiki-NG Version 4.6

1 Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

Changes from Revision * (December 2020) to Revision A (January 2021)	Page
• Updated the numbering format for tables, figures and cross-references throughout the document	1
• Updated 'Affected products and versions' section	1

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265