SECURITY ADVISORY ID:202000401

REV.1.0

DEC.6TH, 2021
RENESAS PSIRT
RENESAS ELECTRONICS CORPORATION

SECURITY ADVISORY [ID:202000401]
VULNERABILITY OF OPEN SOURCE UIP TCP/IP

1.CVEID - CVSS vector - base score

CVEID	CVSS vector	base score
CVE-2020-13984～8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H [7.5]	7.5
CVE-2020-17437	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H [8.2]	8.2
CVE-2020-17438	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H [9.8]	9.8
CVE-2020-17439	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L [8.3]	8.3
CVE-2020-17440	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H [7.5]	7.5
CVE-2020-17441	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H [9.1]	9.1
CVE-2020-17442～5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H [7.5]	7.5
CVE-2020-17467	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H [9.1]	9.1
CVE-2020-17468～9	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H [7.5]	7.5
CVE-2020-17470	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N [5.3]	5.3
CVE-2020-24334	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H [8.2]	8.2
CVE-2020-24336	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H [9.8]	9.8
CVE-2020-24337	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H [7.5]	7.5
CVE-2020-24338	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H [9.8]	9.8
CVE-2020-24339～40	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H [7.5]	7.5
CVE-2020-24341, 383	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H [9.1]	9.1
CVE-2020-25107～12	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H [9.8]	9.8

2. Publication date
Dec 10, 2020

3. Summary

On Wednesday, December 9th, Japan time, a vulnerability was revealed in open source software (uUP TCP / IP protocol stack) that could cause security problems. The identification numbers for the vulnerability-related information related to this matter are as follows:

-JVNVU#96491057
-VU#815128
-ISC-VU-633937

4. Affected products(and versions)
SH7216, H8S/2472, RX62N

5. (Potentially)Impacted features
Application Notes
1. H8S/2472 and SH7216 uIP TCP/IP Protocol Stack Demonstration (Doc#:REU05B0075-0200)
2. RX62N Group uIP TCP/IP Protocol Stack Demonstration (Doc#:R01AN0169EU0101)

6. Suggested fixes/actions/mitigations/remediations
No plan for any fix. Therefore, please refrain from using the above application notes.

7. Source/External references
- uIP https://github.com/adamdunkels/uip
- CERT/CC https://www.kb.cert.org/vuls/id/815128
- ISC-CERT https://us-cert.cisa.gov/ics/advisories/icsa-20-343-01
- JPCERT/CC https://jvn.jp/vu/JVNVU96491057/

Important Notice and Disclaimer

1. No semiconductor product is absolutely secure. Notwithstanding any security measures or features that may be implemented in Renesas hardware or software products, Renesas shall have absolutely no liability arising out of any vulnerability or security breach, including but not limited to any unauthorized access to or use of a Renesas product or a system that uses a Renesas product. RENESAS DOES NOT WARRANT OR GUARANTEE THAT RENESAS PRODUCTS, OR ANY SYSTEMS CREATED USING RENESAS PRODUCTS WILL BE INVULNERABLE OR FREE FROM CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, DATA LOSS OR THEFT, OR OTHER SECURITY INTRUSION ("Vulnerability Issues"). RENESAS DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATED TO ANY VULNERABILITY ISSUES. FURTHERMORE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, RENESAS DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND ANY RELATED OR ACCOMPANYING SOFTWARE OR HARDWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.
2. This document may contain summary of, or excerpts from, certain external websites or sources, which links in this document may connect. Renesas does not manage or have any control over such external websites or sources. Renesas does not warrant or guarantee the accuracy or any other aspect of any information contained in such external websites or sources.