SECURITY ADVISORY ID:202203101

REV.1.00

FEB.20TH, 2023
RENESAS PSIRT
RENESAS ELECTRONICS CORPORATION

SECURITY ADVISORY [ID:202203101]

BUFFER OVERREAD IN DTLS CLIENTHELLO PARSING(CVE-2022-35409, CVSS:9.1 CRITICAL)

1. CVEID – CVSS vector [base score]
   CVE-2022-35409 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H[9.1]

2. Publication date
   Feb. 20th, 2023

3. Summary
   An issue was discovered in Mbed TLS before 2.28.1 and 3.x before 3.2.0. In some configurations, an unauthenticated attacker can send an invalid ClientHello message to a DTLS server that causes a heap-based buffer over-read of up to 255 bytes. This can cause a server crash or possibly information disclosure based on error responses.

4. Affected products (and versions)

Product Family	Software	Version
RX Family	FreeRTOS IoT Integrations	202107.00 (Mbed TLS: 2.16.10)
RL78 Family		202002.00 (Mbed TLS: 2.16.0)
RE Family		202012.00 (Mbed TLS: 2.16.8)

5. (Potentially) Impacted features
   Mbed TLS related S/W used(or implemented) in FreeRTOS.

6. Suggested fixes/actions/mitigations/remediations.
   - RX Family
     https://github.com/renesas/iot-reference-rx
     includes Mbed TLS: 3.2.1 or later
   - RL78 Family
     No update needed. RL78 uses FreeRTOS but TLS process is off-loaded to wireless module.
   - RE Family
     No update.
7. Source/External references
   https://nvd.nist.gov/vuln/detail/CVE-2022-35409

Revision	Remarks	Date
1.0	Initial publication.	Feb.20, 2023

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.