# SECURITY ADVISORY ID:202404401

REV.1.00

MAR. 7TH, 2025
RENESAS PSIRT
RENESAS ELECTRONICS CORPORATION

# SECURITY ADVISORY [ID:202404401]

## FREERTOS-PLUS-TCP CONTAIN A BUFFER OVER-READ ISSUE IN THE DNS RESPONSE PARSER (CVE-2024-38373, CVSS 8.1 HIGH)

1. CVEID – CVSS vector [base score]
   CVE-2024-38373 - CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H[8.1]

2. Publication date
   Mar. 7th, 2025

3. Summary
   FreeRTOS-Plus-TCP is a lightweight TCP/IP stack for FreeRTOS. FreeRTOS-Plus-TCP versions 4.0.0 through 4.1.0 contain a buffer over-read issue in the DNS Response Parser when parsing domain names in a DNS response. A carefully crafted DNS response with domain name length value greater than the actual domain name length, could cause the parser to read beyond the DNS response buffer. This issue affects applications using DNS functionality of the FreeRTOS-Plus-TCP stack. Applications that do not use DNS functionality are not affected, even when the DNS functionality is enabled.

4. Affected products (and versions)

| Product Family | Software | Version |
|---|---|---|
| RZ Family | RZ Family Flexible Software Package (FSP) | RZ/A FSP v3.1.0 and earlier |
| RA Family | RA Family Flexible Software Package (FSP) | FSP v5.4.0 and earlier |

# SECURITY ADVISORY [ID:202404401]

## FREERTOS-PLUS-TCP CONTAIN A BUFFER OVER-READ ISSUE IN THE DNS RESPONSE PARSER (CVE-2024-38373, CVSS 8.1 HIGH)

5. (Potentially) Impacted features
   FreeRTOS-Plus-TCP SW used with FreeRTOS and included in the RZ and RA Family Flexible Software Package (FSP).

6. Suggested fixes/actions/mitigations/remediations.
   - RZ Family
     Update to RZ/A FSP v3.2.0 or later.
   - RA Family
     Update to FSP v5.5.0 or later.

7. Source/External references
   https://nvd.nist.gov/vuln/detail/CVE-2024-38373

| Revision | Remarks | Date |
|---|---|---|
| 1.0 | Initial publication. | Mar. 7, 2025 |
| | | |
| | | |

## 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.