SECURITY ADVISORY ID:202403901

REV.1.00

MAR. 7TH, 2025
RENESAS PSIRT
RENESAS ELECTRONICS CORPORATION

SECURITY ADVISORY [ID:202403901]

ARBITRARY READ AND WRITE DUE TO VULNERABILITY IN PARAMETER CHECKING IN AZURE RTOS THREADX (CVE-2023-48693, CVSS:9.8 CRITICAL)

1. CVEID – CVSS vector [base score]
   CVE-2023-48693 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H [9.8]

2. Publication date
   Mar. 7th, 2025

3. Summary
   Azure RTOS ThreadX is an advanced real-time operating system (RTOS) designed specifically for deeply embedded applications. An attacker can cause arbitrary read and write due to vulnerability in parameter checking mechanism in Azure RTOS ThreadX, which may lead to privilege escalation. The affected components include RTOS ThreadX v6.2.1 and below.

4. Affected products (and versions)

Product Family	Software	Version
RX Family	Azure RTOS Integrations	Release RX MCUs Azure RTOS 2.0.0 comes from original 6.2.1 and earlier
RZ Family	RZ Family Flexible Software Package (FSP)	RZ/A FSP 3.0.0 and earlier
RA Family	RA Family Flexible Software Package (FSP)	FSP v5.3.0 and earlier
Synergy Family	Synergy Software Package (SSP)	SSP 2.6.0 and earlier

SECURITY ADVISORY [ID:202403901]

ARBITRARY READ AND WRITE DUE TO VULNERABILITY IN PARAMETER CHECKING IN AZURE RTOS THREADX (CVE-2023-48693, CVSS:9.8 CRITICAL)

5. (Potentially) Impacted features
   Azure RTOS ThreadX stacks used and included in the software of RX, RZ, RA and Synergy family

6. Suggested fixes/actions/mitigations/remediations.
   - RX Family
     Update to Release RX MCUs Azure RTOS 1.0.0 comes from original 6.4.0 or later
   - RZ Family
     Update to RZ/A FSP 3.1.0 or later
   - RA Family
     Update to FSP v5.4.0 or later.
   - Synergy Family
     Update to SSP 2.6.1 or later

7. Source/External references
   https://nvd.nist.gov/vuln/detail/CVE-2023-48693

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.