SECURITY ADVISORY ID:202400001

REV.1.0

13 MARCH, 2024
RENESAS PSIRT
RENESAS ELECTRONICS CORPORATION

SECURITY ADVISORY [ID: 202400001]
DA1469X SECURE BOOT VULNERABILITIES

1.CVEID - CVSS vector [base score]
CVE-2024-25076 - [Renesas: CVSS:4.0/AV:P/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L 5.4 / medium]
CVE-2024-25077 - [Renesas: CVSS:4.0/AV:P/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L 5.4 / medium]

2.Publication date
Expected Mar 2024.

3.Summary
Renesas have received notification from a 3rd party test house of two vulnerabilities observed in the secure boot process of the DA1469x Bluetooth Low Energy SoC identified in a penetration attack test campaign.

The report has been analysed and the vulnerabilities confirmed. Exploitation of these vulnerabilities severely compromises the secure boot process, meaning that arbitrary third-party (or injected) code be executed even when the secure boot is enabled.

In order to expose these vulnerabilities the attacker must have physical access to the target device, the vulnerabilities cannot be exposed by remote or over-the-air access.

4.Affected products(and versions)
DA1469x family: DA14691, DA14695, DA14697 & DA14699

5.(Potentially)Impacted features
Non-functioning secure boot, possibility to execute malicious code.

6.Source/External references
Not available

7.Acknowledgement
Renesas would like to thank the 3rd party test house for their responsible reporting of their findings.

Revision	Remarks	Date
1.0	Initial publication.	13th Mar, 2024

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.