SECURITY ADVISORY ID:202400002

REV.1.0

12 JUNE 2024
RENESAS PSIRT
RENESAS ELECTRONICS CORPORATION

SECURITY ADVISORY [ID: 202400002]
DA1469X SIGNING KEY MASKING VULNERABILITY

1. CVSS vector [base score]
   [Renesas: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N 8.7 / high]
2. Publication date
   12-Jun 2024
3. Summary
   Ongoing internal continuous improvement work has identified an instance in the Renesas DA1469x / SDK10 where a NONCE (Number Used Once) is stored. In this instance the NONCE is used to mask passkeys, so if exploited can lead to the device security being compromised.
4. Affected products(and versions)
   DA1469x family: DA14691, DA14695, DA14697, DA14699 & DA14695MOD
5. (Potentially)Impacted features
   Exploitation can lead to a malicious party extracting customer application code.
   There is no impact for an end user.
6. Fix
   A new NONCE is created every time a secure image is created.
7. Fix releases
   Hotfixes for SDK10.0.10 & SDK10.0.12 will be available thru the Renesas web portal.

Revision	Remarks	Date
1.0	Initial publication.	12th Jun 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.