SECURITY ADVISORY ID:202500001

REV.1.0

13 MAY 2025
RENESAS PSIRT
RENESAS ELECTRONICS CORPORATION

SECURITY ADVISORY [ID: 202500001]
RL78/G1D ENCRYPTION FAILURE VULNERABILITY

1. CVSS vector [base metrics]
   [Renesas:CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:L/ 3.7 / low]

2. Publication date
   13-May 2025

3. Summary
   In Bluetooth Core Specification, if encryption fails due to the remote device losing bonding information, it states that the local device is recommended to notify the user.
   However, the provided example software is implemented to automatically perform re-pairing without notifying it.
   As a result, a malicious device that spoofs the Bluetooth device address and impersonates the remote device intentionally causes an encryption failure to establish pairing with the local device, and the malicious device gains the right to attack. In addition, the previously paired remote device can no longer be reconnected.

4. Affected products(and versions)

Product	Software (Document number)	Version
RL78/G1D	Bluetooth® Low Energy Protocol Stack Embedded Configuration Sample Program (R01AN3319)	Rev.1.20 and earlier
RL78/G1D	Bluetooth® Low Energy Protocol Stack Fast Prototyping Board Host Sample (R01AN4834)	Rev.1.20 and earlier
RL78/G1D	Bluetooth® Low Energy Protocol Stack Sensor Application (R01AN4159)	Rev.1.03 and earlier

5. (Potentially)Impacted features
   The local device could be spoofed by malicious devices.
   The remote device that was originally paired would not be able to reconnect because the bonding information in the local device would be replaced with a new one.

SECURITY ADVISORY [ID: 202500001]
RL78/G1D ENCRYPTION FAILURE VULNERABILITY

6. Suggested fixes/actions/mitigations/remediations.
   The following document describes how to modify the software to notify a user application of encryption failures.

Product	Software (Document number)	Version
RL78/G1D	Bluetooth® Low Energy Protocol Stack Security Library (R01AN3777)	Rev.1.01

   Users are recommended to modify the software in accordance with the updated document above.

7. Source/External references

   "Action after encryption setup failure" is described in the following specifications.
   Core Specification | Bluetooth® Technology Website
   Volume 3, Part H, Section 2.4.4.2

Revision	Remarks	Date
1.0	Initial publication.	13th May 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.