RENESAS PSIRT SECURITY ADVISORY ID:202100901

REV.1.1

FEB.3RD, 2022
RENESAS PSIRT
RENESAS ELECTRONICS CORPORATION

SECURITY ADVISORY [ID:202100901]
DEVICES SUPPORTING BLUETOOTH CORE AND MESH SPECIFICATIONS ARE VULNERABLE TO IMPERSONATION ATTACKS AND AUTHVALUE DISCLOSURE

1.CVEID - CVSS vector [base score]

CVEID	CVSS vector	base score
CVE-2020-26558	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N	4.2
CVE-2020-26560	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	8.1
CVE-2020-26557	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	7.5
CVE-2020-26556	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	7.5
CVE-2020-26559	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	8.8

*CVE-2020-26555 is not applicable.

2.Publication date
See Item 6.

3.Summary
a. Core
When an attacker makes a man-in-the-middle attack between the pairing initiator and responder in the authentication procedure by Passkey Entry of Bluetooth LE Secure Connections pairing, the attacker estimates the Passkey by using the same public key as the initiator and becomes the initiator resulting in being possible to impersonate.
b. Mesh
In Bluetooth mesh profile specifications v1.0 and 1.0.1, nearby devices that can successfully brute force an AuthValue that is not sufficiently random before the provisioning procedure times out are authenticated by utilizing Malleable Commitments resulting in being possible to complete.

4.Affected products(and versions)
RX23W, RA4W1, RE01B

5.(Potentially)Impacted features
Bluetooth Core and Mesh Specifications.

6.Suggested fixes/actions/mitigations/remediations
- RX23W
  - RX23W Group BLE Module Firmware Integration Technology Application Note - Sample Code | Renesas [21/10/15]
  - RX23W Group Bluetooth Mesh Module Using Firmware Integration Technology Rev.1.20 - Sample Code [21/09/30]
  - RX23W Group Bluetooth Mesh Stack Development Guide Rev.1.20(renesas.com) [21/09/30]
- RA4W1
  - Releases · renesas/fsp · GitHub [21/08/31]
- RE01B
  - RE01B Group Bluetooth Low Energy Sample code (using CMSIS Driver Package) Application Note - Sample Code | Renesas[21/07/30]

7.Source/External references
https://kb.cert.org/vuls/id/799380
http://jvn.jp/vu/JVNVU99594334/

Revision	Remarks	Date
1.0	Initial publication.	Jan.31, 2022
1.1	Dead link fixed.	Feb.03, 2022

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.