SECURITY ADVISORY ID:2020DLG01

REV.1.1

UPDATED 27TH JANUARY 2025
RENESAS PSIRT
RENESAS ELECTRONICS CORPORATION

SECURITY ADVISORY [ID: 2020DLG01] SWEYNTOOTH VULNERABILITY

1. CVE-2019-17517 CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H 5.7 medium
   CVE-2019-17518 CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 6.5 medium

2. Initial Publication date
   28-Feb 2020

3. Summary
   Published as a white paper by the Singapore University of Technology and Design. The white paper and a tool to reproduce this are available at the following link: https://asset-group.github.io/disclosures/sweyntooth/. Renesas Bluetooth devices were included in the investigation and found to be vulnerable to attacks that could force products to reset. The vulnerabilities affecting these devices do not let the attacker inject code into memory to bypass the available Bluetooth security mechanism.

4. Affected products(and versions)
   DA14580/DA14581/DA14583 & DA14680/DA14681/DA14682/DA14683 & DA1469x SDK10.0.4 only

5. (Potentially)Impacted features
   Application interrupted, products reset or denial of service.

6. Fix
   hotfixes & new SDK releases available

7. Fix releases

DA14580/DA14581/DA14583 SDK.3.0.X		hotfix available – contact Renesas Sales
DA14580/DA14581/DA14583 SDK5.0.4		hotfix available online thru product web page
DA14585/DA14586	SDK6.0.12	hotfix available online thru product web page
DA14585/DA14586	SDK6.0.14 & later	fixed in all releases from SDK6.0.14 onwards
DA14680/DA14681/DA14682/DA14683 SDK1.0.14		hotfix available online thru product web age
DA1469x SDK10.0.4		fixed in all releases from SDK10.0.6 onwards

Revision	Remarks	Date
1.0	Initial publication.	28th Feb 2020
1.1	Updated publication.	27th Jan2025

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.