SECURITY ADVISORY ID:202606201

REV.1.0

13 MARCH 2026
RENESAS PSIRT
RENESAS ELECTRONICS CORPORATION

© 2026 Renesas Electronics Corporation. All rights reserved.

SECURITY ADVISORY [ID: 202606201]
RL78 DEBUG PORT SECURITY PROTECTIONS CAN BE BYPASSED BY ATTACKS

1. CVSS vector [base metrics]
   [Renesas:CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H / 6.8 / Medium]
2. Publication date
   13-March 2026
3. Summary
   Security protections of the debug port implemented in the affected products can be bypassed by fault injection attacks. Specifically, protections based on disabling on-chip debug operation and Security ID authentication may be circumvented. In addition, arbitrary code execution may be possible by abusing undocumented commands. Exploitation of this vulnerability requires physical access to the device.
4. Affected products(and versions)
   RL78/G1x series, RL78/L1x series, RL78/I1x series, RL78/H1D, RL78/F1x series, RL78/D1A
5. (Potentially)Impacted features
   Successful exploitation of this vulnerability may lead to the extraction or manipulation of memory contents in the MCU. This may result in loss of confidentiality, integrity, and availability, depending on the system implementation and security requirements.
6. Suggested fixes/actions/mitigations/remediations.
   Renesas recommends applying appropriate system-level countermeasures to make physical access and probing more difficult.
   Details of effective mitigation measures depend on the system design and operational environment.
   Please contact your Renesas sales representatives for further guidance.
7. Source/External references
   CWE-1247: Improper Protection Against Voltage and Clock Glitches
   CWE-1242: Inclusion of Undocumented Features or Chicken Bits

© 2026 Renesas Electronics Corporation. All rights reserved.

Revision	Remarks	Date
1.0	Initial publication.	13th March 2026

© 2026 Renesas Electronics Corporation. All rights reserved.

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.

© 2026 Renesas Electronics Corporation. All rights reserved.