SECURITY ADVISORY ID:202201801

REV.1.2

JUN.28TH, 2022
RENESAS PSIRT
RENESAS ELECTRONICS CORPORATION

SECURITY ADVISORY [ID:202201801]
APACHE LOG4J SECURITY VULNERABILITY

1.CVEID - CVSS vector [base score]

CVE-2021-44228 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H[10.0]
CVE-2021-45105 - CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H[5.9]
CVE-2021-45046 - CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H[9.0]

2.Publication date

Jan 31st, 2022

3.Summary

Apache Log4j is an open source Java-based logging library provided by the Apache Software Foundation.
There is a possibility that an arbitrary command can be executed by sending a specially crafted data by a remote third party in this Apache Log4j which has a function called Lookup that replaces some strings as variables from the strings recorded as logs.
When the JNDI Lookup function is exploited, a remote third party sends a specially crafted character string and Log4j records it as a log, so that Log4j is a java class from the communication destination or internal path specified by Lookup. It can read and execute the file and result in arbitrary code execution.
Renesas continue monitoring this issue and will update when needed.

4.Affected products(and versions)

No product affected.

5. Source/External references

Log4j – Apache Log4j Security Vulnerabilities

Revision	Remarks	Date
1.0	Initial publication.	Jan.31, 2022
1.1	Dead link fixed.	Feb.03, 2022
1.2	Footer corrected(No contents changed).	Jun.28, 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.