RIMAGE®

Security Bulletin – Dec 14, 2021

Apache Log4j Library Critical Remote Code Execution Vulnerability

CVE-2021-4422 aka "Logjam"

The NIST has published notice of a critical vulnerability in software that utilizes the Apache log4j library version 2.14.1 or earlier. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

While the RSS and RAS suites do not utilize the affected library, the WebRSM software included with RSS up to and including version 9.1 is affected.

Rimage recommends taking the steps below to eliminate this attack vector:

- **If possible, update your RSS software to 9.4.x.**
- **Uninstall the WebRSM software if it is currently installed.**

If you have questions or require support on this topic, please contact Rimage Technical Support for assistance.

Email: support@rimage.com

Phone: **Americas:** **+1-800-553-8312 #2**
Europe: **+49 6074.8521 – 14**

More details and ongoing updates on this issue can be found at the NIST link below.
https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Rimage Corporation
201 General Mills Boulevard
Minneapolis, MN 55426 USA
Toll Free: 1-800-445-8288