Customer Information Bulletin – CIB1501 – Log4Shell vulnerability

Subject

A vulnerability has been discovered in the Log4j tool which is a Java-based logging utility developed by Apache. This Customer Information Bulletin gives information about what this means for the Rohill products.

Description

This Log4Shell vulnerability has been reported as CVE-2021-44228. When an application that is making use of Log4j is accessible via the internet and inbound requests from the internet are possible, a hacker might get root access to the server which runs the application.

Impact

When a hacker has got root access to the server, the hacker has access to the data on that server, can potentially access other servers in the network and may install malware or perform a ransomware attack.

Detection

None of the products of the Rohill product portfolio are making use of Log4j and thus are not affected by this Log4Shell vulnerability.

Affected Versions

None.

Solution

Not applicable.

More information

Please contact the Technical Support department of Rohill when more information is required.
Email address: support@rohill.nl.