

# Exalate Response to Log4j Vulnerability - CVE-2021-44228

Last Modified on 01/28/2026 1:57 pm EST

On Saturday, December 10, 2021 - we were made aware of the Log4j vulnerability in the apache logging framework ([CVE-2021-44228](#)), ([CVE-2021-45046](#)), and ([CVE-2021-45105](#)).

The results of our investigation are that Exalate is **NOT** affected by this vulnerability as Exalate is using [ch.qos.logback](#) on all Exalate products (except for Exalate for Jira On Premise)

There **might** be a risk for 'Exalate for Jira On Premise', which is using the logging framework provided by Jira.

Atlassian confirmed [here](#) that Jira itself is not vulnerable but the advice is to check for 'org.apache.log4j.net.JMSAppender' in the log4j.properties file.

[About Us](#) ?

[Release History](#) ?

[Glossary](#) ?

**Note:** [API Reference](#) ?

[Security](#) ?

[Pricing and Licensing](#) ?

## Resources

[Subscribe for a weekly Exalate hack](#) ?

[Academy](#) ?

[Blog](#) ?

[YouTube Channel](#) ?

[Ebooks](#) ?

## Still need help?

[Join our Community](#) ?

[Visit our Service Desk](#) ?

[Find a Partner](#) ?