17/12/2021 15:25

Log4J FAQ

Log4J zero-day vulnerability

A zero-day vulnerability CVE-2021-44228 has been found in relation to Log4J.
Log4J is commonly used for handling logging in Java based systems.

You should use this FAQ as starting point for any questions you might have. If your question is not covered, please raise a ticket in the Service Portal.

Contents

Is STEP affected by CVE-2021-44228?

STEP is using a version of Log4J that is not affected. I.e., STEP is not affected by the CVE-2021-44228 vulnerability.

Do Stibo Systems plan to update to the latest version of Log4J?

A: We're investigating what side-effects an upgrade can have. If it is possible, STEP 11 will be released with the latest version of Log4J (2.16.0).

Why is Stibo running older versions of the Log4J?

A: Stibo Systems has a very effective Third-Party governance program, as part of our ISO 27001 certified Secure Development Policy. We only allow certain versions of certain libraries into our product. Only when new libraries have been properly approved is it possible to use them in the product source code.

Furthermore, all approved and used libraries are being scanned daily against the National Vulnerability Database, hosted by the US government. If new vulnerabilities are found in any of the used libraries, the identified problems are assessed, and upgrade plans are made depending on the severity of these findings. Not all vulnerabilities are grave enough to warrant upgrading to the newest version of a library, which is more likely to include yet unknown problems. For that reason, we do not upgrade libraries that do not need to be upgraded.

The MDM Platform source code uses 100s of third-party libraries. Unfortunately, the dependency graph doesn't only point from our code to third party software, but also from one third party library to another. This makes the upgrade process complex.

We've known for many years that the Log4J library wasn't up to date, but because of a third-party dependency on Log4J, we were not able to upgrade the library. But because we did a thorough analysis of the usage of the logging framework, we have concluded that we aren't vulnerable to any of the three known CVEs associated with the version we're running.

By not being overly aggressive with our upgrade strategy, we saved ourselves and our customers from a very serious vulnerability that could have had grave implications to the stability and security of a STEP installation. This does not mean that we do not have a well-defined upgrade strategy, as outlined above.

Is STEP affected by CVE-2019-17571?

A: No, STEP does not use the SocketServer class, which means that STEP is not affected by this CVE.

Is STEP affected by CVE-2021-4104?

A: No, STEP is not setup per standard to use JMS Appender.

Is Stibo's PDX solution affected by CVE-2021-44228?

A: No, the PDX java services use **logback** as the actual logging engine.

Are there any changes needed with Elastic search?

A: For Stibo SaaS customers needed configuration changes have already been applied, but on-premises customers should set this jvm parameter: -DLog4J2.formatMsgNoLookups=true.

In the Oracle installation I found Oracle client jars with names that point to Log4J. Are they a risk too?

A: Only server components using Log4J are vulnerable. Client programs cannot be accessed from the outside.
If the attacker is able to launch your client program, this person has already all the access he needs.

Is STEP affected by CVE-2021-45046?

A: STEP is not using a version of Log4J that is vulnerable to this CVE.