Oracle Database and Apache log4j vulnerability CVE-2021-44228 and CVE-2021-45046 (Doc ID 2828877.1)

In this Document

APPLIES TO:

Oracle Database - Enterprise Edition - Version 11.2.0.4 and later
Oracle Database - Standard Edition - Version 11.2.0.4 and later
Information in this document applies to any platform.

MAIN CONTENT

This note also applies to the Oracle Grid Infrastructure – version 11.2.0.4 and later

GOALS:

Discuss Oracle Database and CVE-2021-44228 / CVE-2021-45046, a remote code execution in Apache log4j.

IMPORTANT INFORMATION:

Oracle Security Alert Advisory - CVE-2021-44228 discusses this vulnerability and affected Oracle products. My Oracle Support (MOS) document id 2827611.1 details the comprehensive list of Oracle products and versions impacted by these vulnerabilities, and also identifies those Oracle products that are not impacted by the vulnerabilities.

This document discusses the vulnerabilities as it relates to the Oracle Database and contains information that supplements the contents of MOS document id 2827611.1.

Oracle Database (all supported versions including 11.2, 12.1, 12.2, 19c, and 21c) are not affected by vulnerability CVE-2021-44228 or CVE-2021-45046.

There are two versions of log4j. Log4j version 1 (log4jv1) is not impacted by CVE-2021-44228 or CVE-2021-45046. Only log4j version 2 (log4jv2) is impacted by CVE-2021-44228 or CVE-2021-45046. There is another log4j vulnerability, CVE-2021-4104, that does impact log4jv1. That vulnerability is only exploitable if a non-default log4j configuration enables a JMSAppender that is allowed to perform JNDI requests. The Oracle Database's use of log4jv1 does not use a JMSAppender, and the Oracle Database is evaluated as not vulnerable to CVE-2021-4104.

Log4jv2 was used by Parallel Graph Analytics (PGX) and appeared in the $ORACLE_HOME/md/property graph directory. Log4jv2 was removed with the October 2020 release update. PGX is not configured by default and must be manually deployed in a Java container.

Oracle Databases with the October 2020 or later critical patch update are evaluated as not vulnerable to CVE-2021-44228 or CVE-2021-45046

Log4jv2 was part of Oracle Spatial, and was present in $ORACLE_HOME/md/jlib directory. This was a dependency of a component in the Oracle Spatial and Graph Network Data Model (NDM) Server. The NDM Server is not configured by default and must be manually deployed in a Web Logic Server (WLS) container by customers wishing to use it. Even when deployed, no logging was done through the log4j library – there is no code execution path that calls the impacted library. For this reason, even databases with NDM deployed in a WLS are evaluated as not vulnerable to CVE-2021-44228 or CVE-2021-45046. For customers concerned about the presence of the log4j files, patch 33674035 removes the unused log4jv2 files. The October 2021 critical patch update also removes these files.

Trace File Analyzer (TFA) which is part of the Autonomous Health Framework (AHF) uses log4jv2. If you are using TFA, you should download version 21.3.4 or higher. The log4j-*.jar files in $ORACLE_HOME/suptools/tfa/release/tfa_home/jlib directory are no longer used once version 21.3.4 is installed. The log4j files were removed from $ORACLE_HOME with the July 2021 grid and database release update. MOS document id 2550798.1 has more information about CVE-2021-44228 and TFA, including links to download the latest version. The latest version of AHF is also downloadable as patch 30166242. Installations of the Autonomous Health Framework with versions earlier than 21.3.4 are evaluated as vulnerable unless the July 2021 or later release update is installed and the AHF version is updated to at least 21.3.4. To determine your TFA version, execute:

$AHF_HOME/bin/tfactl -version

AHF installations 21.3.4 and above are evaluated as not vulnerable to CVE-2021-44228 or CVE-2021-45046

Note: Scans for the log4jv2 files may find them in $ORACLE_HOME/.patch storage. This directory is used to un-install a patch. Files in this location are never accessed by the running database processes.

RECOMMENDATIONS:

If you have not already installed the October 2020 release update/critical patch update you should evaluate your risk exposure to CVE-2021-44228 and CVE-2021-45046

If you are using Trace File Analyzer, you should download version 21.3.4 or higher (see MOS document ID 2550798.1). If you have not yet installed the July 2021 release update/critical patch update you should evaluate your risk exposure to CVE-2021-44228 CVE-2021-45046

Continue to monitor this document and document id 2827611.1 for updates.

FOR MORE INFORMATION:

Oracle Security Alert Advisory - CVE-2021-44228

document id 2827611.1 Apache Log4j Security Alert CVE-2021-44228 Products and Versions

document id 2550798.1 Autonomous Health Framework (AHF) - Including TFA and ORAchk/EXAchk

Oracle Database Licensing Information User Manual – Third-party notices and/or licenses for Oracle Database components

Didn't find what you are looking for?