# AP Tools log4j Impact

**JANUARY 2022**

SECURE CONNECTIONS
FOR A SMARTER WORLD

# AP TOOLS LOG4J VULNERABILITY IMPACT

A vulnerability in the Apache log4j was identified in the articles: CVE-2021-44228 and CVE-2021-45046
AP SW Tools team has performed an analysis of this vulnerability, below is a summary of the result.

| Tool | Impact | Details |
|---|---|---|
| S32 Design Studio<br>• S32 Platform<br>• Arm<br>• Power | None | The S32 Design Studio (all versions) is **NOT IMPACTED**. Although the Log4j is used by S32 Design Studio, the version used is 1.x and the vulnerability was introduced in version 2.12 with a combination of Java versions 9/10/11 where LDAP policy is enabled by default (CVE-2021-45046). The S32Design Studio installation environment is independent and based on Java 8 version, which is common for all tools running under S32Design Studio IDE. In addition, the S32 Design Studio does not use JMSAppender, so it is not affected by the identified log4j 1.x usage concern (CVE-2021-44228). When we determine an upgrade of the Log4j and/or Java version is required for a future release of S32 Design Studio, then this vulnerability will be addressed. |
| S32 Flash Tool | None | S32 Flash Tool does not contain log4j |
| S32V2 DDR Stress Test and Validation Tool | None | It is command line, without Java |
| Model-Based Development Tools | None | There is no impact on MBDT because it has no Java components, that could, potentially, be using log4j. |
| QKit | None | we are using log4j 1.2.15 not log4j 2.x<br>Our version of log4j is only affected if you are using a specific configuration, please see https://logging.apache.org/log4j/2.x/security.html.<br>As we do not use the mentioned **JMSAppender** in our built products/QST/TCA users are not affected as long as users do not modify this configuration. Nevertheless we are currently upgrading to a not vulnerable version of log4j which will be included in one of the upcoming releases of TCA/QST. |
| Legacy Tools<br>• CodeWarrior for MCU<br>• RAppID Init<br>• RAppID Toolbox<br>• RAppID Bootloader<br>• GTM Config Tool<br>• Metrowerks tools<br>• HiWare tools | None | These tools either used much older versions of the Java (version 8 or older) or did not use Java at all, so the log4j vulnerability was either not introduced yet or not possible (CVE-2021-45046). In addition, these tools do not use JMSAppender, so they are not affected by the identified log4j 1.x usage concern (CVE-2021-44228). |

SECURE CONNECTIONS
FOR A SMARTER WORLD