Log4J Vulnerabilities - Kaspersky Resolutions (Updated to 11 Dec 2021)

The information provided below is referred from https://www.kaspersky.com/blog/log4shell-critical-vulnerability-in-apache-log4j/43124/.

- **CVE Number**

  2021-44228

- **Discovery Date**

  Dec 11, 2021

- **Threat Level**

  High

- **Response to Log4j**

Various information security news outlets reported on the discovery of critical vulnerability CVE-2021-44228 in the Apache Log4j library (CVSS severity level 10 out of 10). Millions of Java applications use this library to log error messages. To make matters worse, attackers are already actively exploiting this vulnerability. For this reason, the Apache Foundation recommends all developers to update the library to version 2.15.0, and if this is not possible, use one of the methods described on the Apache Log4j Security Vulnerabilities Page.

Kaspersky recommends to install the Kaspersky Solutions on your servers — in many cases this will allow you to detect the launch of malicious code and stop the attack's development.

- **Affected Kaspersky Products**

Kaspersky products are not affected by the CVE-2021-44228 vulnerability.