Critical Vulnerability in Log4j

A CRITICAL VULNERABILITY WAS DISCOVERED IN THE APACHE LOG4J PROJECT (CVE-2021-44228)

Last Friday a critical vulnerability was discovered in the Apache log4j project (CVE-2021-44228). For software using the library, simply logging a string of a specific format can lead to remote code execution. Log4j 2.15 fixes this issue, we advise our users to update their affected products as soon as possible.

We conducted an in-depth review and can confirm that products and services provided by Devolutions are **not affected** by this vulnerability.

Details and Mitigation

LunaSec published a great explanation of how this vulnerability can be exploited if you are interested in the details. The gist of it is that simply by logging a string in a specific format, a vulnerable application can be made to download and execute arbitrary code from a remote LDAP server. Because log4j is the de facto logging library for Java applications, a very large number of systems and services are affected.

Projects using log4j should update to version 2.15 as soon as possible. The log4j project also provides other mitigation steps.

We also advise our users to update their systems that are affected by this vulnerability. The Nationaal Cyber Security Centrum published a list with the vulnerability status for products of major vendors.

https://github.com/NCSC-NL/log4shell/tree/main/software