LEYARD™

eyevis
A LEYARD Company

Europe, Hundsschleestrasse 23, 72766 Reutlingen, Germany
+49 7121 433030
www.leyard.com | www.eyevis.de

Reutlingen, 15/12/2021

To whom it may concern

Apache Log4j is a library for logging functionality in Java-based applications.

A flaw was found in Apache Log4j, allowing a remote attacker to execute code on the server if the system logs an attacker-controlled string value with the attacker's Java Naming and Directory Interface™ (JNDI) Lightweight Directory Access Protocol (LDAP) server lookup. This flaw allows a remote attacker to execute code on the target system with the same privileges as the Java-based application that invoked Apache Log4j.

The conditions to exploit this library and its severities are different and based on the version of Apache Log4j.

The first issue is assigned CVE-2021-44228 (Log4j v2.x) and has a severity impact rating of Critical.

The second issue is assigned CVE-2021-4104 (Log4j v1.x) and has a severity impact rating of Moderate.

The eyevis™ eyeUNIFY products are **NOT** affected by this flaw and have been explicitly listed here for the benefit of our customers.

- eyevis™ eyeUNIFY v1
- eyevis™ eyeUNIFY v2

IN WITNESS WHEREOF, Mr. Cris Tanghe signed this instrument on
Wednesday, December 15, 2021

Cris Tanghe
VP Product Europe
Leyard s.r.o