PROGNOST
INTELLIGENCE ON DUTY

Part of the Burckhardt Compression Group

IT-SECURITYINFORMATION

ASSESSMENT OF THE LOG4J TOPIC

INFLUENCES FOR THE IT-SECURITY OF PROGNOST

December 14th, 2021

BACKGROUND INFORMATION

Now that the German Federal Office for Information Security (BSI) has upgraded the threat level of the LOG4J vulnerability (CVE-2021-44228), which was disclosed last week, to red, the implications of this vulnerability for businesses around the world are becoming increasingly clear.

PROBLEM DESCRIPTION

LOG4J is a popular logging library for Java applications. It is used for high-performance aggregation of log data from an application.

LOG4J is used in many Java applications. The protection against active, broad exploitation of the vulnerability is very low due to the availability of a PoC.

IMPACTS IN RELATION TO PROGNOST SYSTEMS

PROGNOST® Applications

- PROGNOST applications do not contain any Java components, so the LOG4J threat can be 100% excluded here.

PROGNOST® Unit - MAPROG30 and APLPROG40x

- No Java services are active on the above-mentioned PROGNOST units, so the LOG4J threat can be 100% ruled out here.

PROGNOST® Unit - MAPROG2 to MAPROG22

- Only the Java application WEBPAM is active on the above-mentioned PROGNOST devices, but it does not use any LOG4J elements, so the LOG4J threat can be ruled out 100%.

FINAL ASSESSMENT

Since, as mentioned above, no LOG4J services or elements are used within the PROGNOST systems, a threat to the PROGNOST systems can be ruled out 100%.

CONTACT

PROGNOST Systems GmbH
Daimlerstr. 10
48432 Rheine
Germany

Phone: +49 5971 80 81 90
Email: info@prognost.com
www.prognost.com