PROGNOST
INTELLIGENCE ON DUTY

Part of the Burckhardt Compression Group

IT-SICHERHEITSINFORMATION

BEURTEILUNG DER **LOG4J THEMATIK**

BEEINFLUSSUNG DER IT-SICHERHEIT VON PROGNOST

14. Dezember 2021

HINTERGRUND

Nachdem das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Bedrohungsgrad der letzte Woche bekanntgewordenen Sicherheitslücke Log4j (CVE-2021-44228) auf Rot heraufgestuft hat, werden die Folgen dieser Schwachstelle für Unternehmen auf der ganzen Welt immer deutlicher.

PROBLEMBESCHREIBUNG

LOG4J ist eine beliebte Protokollierungsbibliothek für Java-Anwendungen. Sie dient der performanten Aggregation von Protokolldaten einer Anwendung.

LOG4J wird in vielen Java-Anwendungen eingesetzt. Der Schutz gegen eine aktive, breite Ausnutzung der Schwachstelle ist durch die Verfügbarkeit eines PoC sehr gering.

EINFLÜSSE IN BEZUG AUF PROGNOST SYSTEME

PROGNOST® Anwendungen

- In den PROGNOST Anwendungen sind keine Java Komponenten enthalten, somit ist die LOG4J Gefährdung hier zu 100% auszuschließen.

PROGNOST® Unit - MAPROG30 und APLPROG40x

- Auf den oben genannten PROGNOST Geräten sind keine Java Dienste aktiv, somit ist die LOG4J Gefährdung hier zu 100% auszuschließen.

PROGNOST® Unit - MAPROG2 bis MAPROG22

- Auf den oben genannten PROGNOST Geräten ist nur die Java Anwendung WEBPAM aktiv, diese nutzt aber keinerlei LOG4J Elemente, somit ist die LOG4J Gefährdung zu 100% auszuschließen.

ABSCHLIESSENDE EINSCHÄTZUNG

Da wie oben genannt, keinerlei LOG4J Dienste oder Elemente innerhalb der PROGNOST Systeme verwendet werden, ist eine Gefährdung der PROGNOST Systeme zu 100% auszuschließen.

KONTAKT

PROGNOST Systems GmbH
Daimlerstr. 10
48432 Rheine
Deutschland

Telefon: +49 5971 80 81 90
E-Mail: info@prognost.com
www.prognost.com