Produktinformation
Stellungnahme zur kritischen Schwachstelle in log4j

Aktuelle Situation

Am 12.12.2021 hat das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Cyber Sicherheitswarnung „Kritische Schwachstelle in log4j veröffentlicht (CVE-2021-44228)“ an die Öffentlichkeit weitergegeben.

Hintergrund

In der Sicherheitswarnung heißt es:
„Log4j ist eine beliebte Protokollierungsbibliothek für Java-Anwendungen. Sie dient der performanten Aggregation von Protokolldaten einer Anwendung.
Das Blog eines Dienstleisters für IT-Sicherheit [LUN2021] berichtet über die Schwachstelle CVE-2021-44228 [MIT2021] in log4j in den Versionen 2.0 bis 2.14.1,
die es Angreifern gegebenenfalls ermöglicht, auf dem Zielsystem eigenen Programmcode auszuführen und so den Server zu kompromittieren…“
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=3

Die Gefahr, dass diese Schwachstelle für Cyber-Angriffe ausgenutzt wird, ist durchaus realistisch, daher schätzt das BSI die Warnstufe mit „4/Rot“ ein.
So wäre beispielsweise ein Angriff über eine Eingabemaske bei der Besucheranmeldung, Urlaubsanträgen, Zeitkorrekturen etc. denkbar, da diese in der Regel protokolliert werden. Beispielsweise könnte ein Angreifer statt eines Namens, direkt ausführbaren Programmcode eingeben und damit unbemerkt Schadsoftware installieren.

Maßnahmen

Die Veröffentlichung hat verständlicherweise zu starker Verunsicherung bei unseren Kunden und Partnern geführt. Wir haben umgehend alle unsere Java-basierenden EAD Softwaresysteme überprüft und möchten kurz über die Ergebnisse in dieser Produktinformation informieren:

dormakaba EAD Lösungen

exos
Alle Versionen sind **nicht betroffen**.
exos basiert nicht auf der Programmiersprache Java. Es wurden aber zwischenzeitlich Programmteile, wie beispielsweise der „Mobile Credential Calculator“, mittels Java Code integriert. Diese Programmteile verwenden die betroffenen log4j Bibliotheken nicht.

MATRIX PRO / ONE
Alle Versionen sind **nicht betroffen**.
Die log4j Bibliothek in den Versionen 2.0 bis 2.14.1 wurde in keiner MATRIX Version verwendet.

KEM
Alle Versionen sind **nicht betroffen.**
KEM ist keine Java Applikation und damit generell nicht von der Sicherheitslücke betroffen.

B-COMM
Die Überprüfung aktueller Versionen >5.0.0 hat ergeben, dass **keine** der betroffenen Funktionen standardmäßig verwendet werden.
Stichproben von älteren Versionen wie 3.18.x und 4.1.3 haben ebenfalls bestätigt, dass **keine** der betroffenen Funktionen verwendet werden.
Hinweis: Da es sich bei B-COMM nur um eine Middleware, die von Partnern zur Anbindung von Geräten genutzt wird, handelt, kann hier keinerlei Aussage über das Gesamtsystem getroffen werden.

b-comm ERP
Alle Versionen sind **nicht betroffen**.
b-comm ERP verwendet die betroffene Bibliothek, aber **keine** der betroffenen Funktionen (inklusive TRS und File-Transceiver).

EACM
Alle Versionen sind **nicht betroffen**.
EACM ist keine Java Applikation und damit generell nicht von der Sicherheitslücke betroffen.

jay cloud
Die Cloudanwendung jay cloud ist **nicht betroffen**.
Die IoT- Anbindung basiert auch auf Java. Die log4j Bibliothek in den Versionen 2.0 bis 2.14.1 wurde nicht verwendet.

evolo smart
Alle Versionen sind **nicht betroffen**.
evolo smart ist keine Java Applikation und damit generell nicht von der Sicherheitslücke betroffen.

mobile access app
Alle Versionen sind **nicht betroffen**.
mobile access app ist keine Java Applikation und damit generell nicht von der Sicherheitslücke betroffen.

Terminals
Die die Terminals B-eco, 93 00, 95 00, 96 00 und 97 00 sind **nicht betroffen**.

Online-Geräte
Online-Geräte (Access Manager mit exos, TP4 und AC30 Client) sind **nicht betroffen**. Auch der Wireless Gateway ist **nicht betroffen**.

dormakaba digital Lösungen

exivo / resivo
Die Cloudanwendungen exivo / resivo sind **nicht betroffen**.

dormakaba Lodging Lösungen

System 6000, Atlas, Ambiance
Die Hotelanwendungen System 6000, Atlas und Ambiance sind **nicht betroffen**.
Bereits gestern haben die Kollegen über eine gesonderte Meldung darüber informiert, dass die log4j Bibliothek in den Lösungen nicht verwendet wird.

Handlungsempfehlung

Basierend auf den Untersuchungsergebnissen sind in Bezug auf die „Kritische Schwachstelle in log4j“ **keine** Maßnahmen erforderlich, die Sicherheit der Lösungen ist durch die Sicherheitslücke **nicht** beeinträchtigt.
Bitte beachten Sie: Unsere Softwarelösungen bieten allgemein die Möglichkeit, Fremdsoftware und Fremdgeräte anzubinden. Bitte haben Sie Verständnis, dass wir keine Aussage über Schnittstellen angebundene Fremdsoftware sowie Fremdprodukte treffen können.

Wir empfehlen generell unseren Kunden und Partnern, für den bestmöglichen Schutz vor Cyberangriffen, ihr System und ihre Hardware regelmäßig auf den neusten Stand zu aktualisieren.

Informationen

Sollten Sie Fragen oder weitere Informationen benötigen, steht Ihnen Ihr Product Management EAD Systems, gerne zur Verfügung.

.

Kontakt

Felix Hoellt
Deputy Vice President
Product Management EAD Systems
felix.hoellt@dormakaba.com
+49 2333 793 6535