Kritiek beveiligingslek in log4j

Huidige situatie

Op 12 december 2021 heeft het Duitse federale bureau voor informatiebeveiliging (BSI) de cybersecurity waarschuwing "Kritieke beveiligingslek in log4j gepubliceerd (CVE-2021-44228)" uit laten gaan.

Achtergrond

De veiligheidswaarschuwing luidt:

"Log4j is een populaire logging bibliotheek voor Java applicaties. Het wordt gebruikt om loggegevens van een applicatie op een efficiënte manier te aggregeren.

De blog [LUN2021] van een IT-beveiligingsserviceprovider meldt kwetsbaarheid CVE-2021-44228 [MIT2021] in log4j versies 2.0 tot en met 2.14.1, waardoor aanvallers hun eigen programmacode op het doelsysteem kunnen uitvoeren en zo de server kunnen compromitteren ..."

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=3

Een update meldt dat de kwetsbaarheid ook geldt voor log4j versies 1.x.

Het risico dat deze kwetsbaarheid wordt misbruikt voor cyberaanvallen is zeer waarschijnlijk, daarom beoordeelt de BSI het waarschuwingsniveau als "4/Red". Zo zou een aanval via een invoerscherm bij bezoekersregistratie, vakantieaanvragen, tijdcorrecties, etc. denkbaar zijn, aangezien deze meestal worden gelogd. Een andere manier waarop het systeem kan worden misbruikt, is dat een aanvaller in plaats van een naam in te voeren, rechtstreeks een executable programmacode kan invoeren en zo onopgemerkt malware kan installeren.

Maatregelen

De veiligheidswaarschuwing heeft begrijpelijkerwijs geleid tot bezorgdheid bij onze klanten en partners. In reactie op de veiligheidswaarschuwing hebben we onmiddellijk al onze op Java gebaseerde EAD-softwaresystemen beoordeeld en willen we al onze belanghebbenden kort informeren over de resultaten van interne beoordeling in deze productinformatieverklaring:

dormakaba EAD Oplossingen

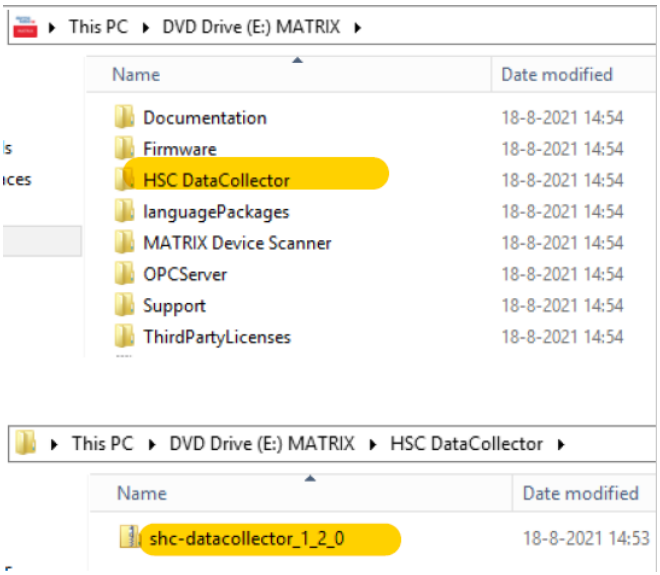
exos

Geen enkele versie wordt hierdoor getroffen.
exos is niet gebaseerd op de programmeertaal Java. Hoewel sommige programmaonderdelen, zoals de "Mobile Credential Calculator", zijn geïntegreerd met behulp van Java-code, gebruiken deze programmaonderdelen niet de getroffen log4j-bibliotheken.

MATRIX PRO / ONE

Bij MATRIX wordt het programma SHC datacollector meegeleverd, welke gebruik maakt van een kritische log4j 2.12.x bibliotheek. Het wordt gebruikt als systeemanalysetool. Het wordt bij installatie

van MATRIX niet mee geïnstalleerd en is ook niet essentieel voor de werking van MATRIX. Het kan handmatig worden gestart. We adviseren je aan de map met het bestand uit de installatiebestanden te verwijderen. De map heet “SHC DataCollector“ of “HSC DataCollector”, het bestand heet shc-datacollector_*. Zie het voorbeeld hieronder.



Alle huidig ondersteunde MATRIX versies gebruiken Log4j version 1.2.13. De kwetsbaarheid waar BSI aan refereert, beïnvloedt het JMSAppender component in log4j. Om kwetsbaar te zijn moet JMSAppender expliciet en specifiek geconfigureerd worden, in tegenstelling tot de default configuratie. MATRIX wordt **niet getroffen** door deze kwetsbaarheid omdat JMSAppender in geen enkele versie van MATRIX wordt gebruikt.

KEM

Geen enkele versie wordt hierdoor getroffen.
KEM is geen Java-applicatie en wordt dus niet getroffen door het beveiligingslek.

B-COMM

Uit een steekproef van de huidige versies >5.0.0 is gebleken dat **geen** van de getroffen functies standaard wordt gebruikt.

Steekproefsgewijze controles van oudere versies zoals 3.18.x en 4.1.3 hebben ook bevestigd dat **geen** van de getroffen functies wordt gebruikt.

Opmerking: Aangezien B-COMM slechts middleware is dat door partners wordt gebruikt om apparaten te koppelen, kan hier geen uitspraak worden gedaan over het algehele systeem.

b-comm ERP

Geen enkele versie wordt hierdoor getroffen.
b-comm ERP maakt gebruik van de betreffende bibliotheek, maar niet van de getroffen functies (inclusief TRS en file transceiver).

EACM

Geen enkele versie wordt hierdoor getroffen.
EACM is geen Java-toepassing en wordt daarom niet getroffen door het beveiligingslek.

Jay Cloud

De cloudapplicatie jay cloud wordt **niet** hierdoor getroffen.
Hoewel de IoT-verbinding ook op Java is gebaseerd, werd de log4j-bibliotheek in versies 1.x, 2.0 tot en met 2.14.1 niet gebruikt.

Evolo smart

Geen enkele versie wordt hierdoor getroffen.
evolo smart is geen Java-applicatie en wordt daarom niet getroffen door het beveiligingslek.

mobile access app

Geen enkele versie wordt hierdoor getroffen.
De mobile access app is geen Java-toepassing en wordt dus niet getroffen door het beveiligingslek.

Terminals

De B-eco, 93 00, 95 00, 96 00 en 97 00 terminals worden **niet** hierdoor getroffen.

Online componenten

Online componenten (Access Manager met exos, TP4 en AC30 Client) worden **niet** hierdoor getroffen. De draadloze gateway wordt ook **niet** getroffen.

dormakaba Digitale Oplossingen

exivo / resivo

De cloudapplicaties exivo / resivo worden **niet** hierdoor getroffen.

dormakaba hoteloplossingen

System 6000, Atlas, Ambiance

De hotelapplicaties System 6000, Atlas en Ambiance worden **niet** getroffen.
De log4j-bibliotheek wordt niet gebruikt in deze oplossingen.

Aanbevolen actie

Los van de aanbeveling ten aanzien van MATRIX ONE en PRO is op basis van de resultaten van het onderzoek geen actie nodig met betrekking tot de "Kritieke kwetsbaarheid in log4j". De beveiliging van de oplossingen van dormakaba wordt niet getroffen door het beveiligingslek.

Let op: onze softwareoplossingen bieden over het algemeen de mogelijkheid om te worden gekoppeld aan software van derden en met componenten van derden. We kunnen geen uitspraken doen over interfaces die zijn gekoppeld met software of producten van derden. Ook over

uitgefaseerde producten en software kunnen we geen uitspraken doen, omdat ze niet meer beschikbaar voor ons zijn.

We raden onze klanten en partners aan om hun systeem en hardware bij te werken naar de nieuwste versie voor de best mogelijke bescherming tegen cyberaanvallen.

Op basis van alle berichtgeving over log4j hebben we besloten om in alle nieuwe leveringen de nieuw gereleaste versie log4j 2.16 als default te gebruiken. We informeren je zo snel mogelijk zodra de nieuwe software packages beschikbaar zijn.

Informatie

Mocht u vragen hebben of meer informatie wensen, aarzel dan niet om contact op te nemen met uw vaste dormakaba accountmanager voor toegangscontrole oplossingen.

dormakaba Nederland B.V.
Dalwagen 45
6669 CB Dodewaard
088-352 33 33
info.nl@dormakaba.com
www.dormakaba.nl