CVE-2021-44228 Sicherheitslücke

Massive und gefährliche IT-Sicherheitslücke - Factsheet Apache Log4j

Sehr geehrte Damen und Herren,

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte ein Schreiben zu einer sehr bedrohlichen Sicherheitslücke in der Open Source Software Apache Log4j (CVE-2021-44228).

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

Die Sicherheitslücke hat einen Gefährdungswert: 10 von 10

Beschreibung

log4j ist ein Framework zum Loggen von Anwendungsmeldungen in Java. Innerhalb vieler Open-Source- und kommerzieller Softwareprodukte hat es sich über die Jahre zu einem De-facto-Standard entwickelt.
Betroffen sind alle Versionen ab Version2.0-beta bis 2.15. Erst die Version 2.16 ist nicht mehr anfällig.

Was bedeutet das im Klartext:

Aktuell versuchen Hacker aus aller Welt aus dem Internet erreichbare Systeme automatisch zu Scannen um die Schwachstelle aufzuspüren. Jeder IT-Anwender wird von diesen Scans betroffen sein.

Die schlechte Nachricht:

Eines der größten Probleme dieser Sicherheitslücke ist ihre Verbreitung. Log4J Bibliotheken (bzw. das Framework) werden von so gut wie jedem Softwarehersteller genutzt. Das bedeutet, dass nicht nur die von uns betreute Basis ihrer IT betroffen ist, sondern vermutlich auch viele der Programme, die Sie im täglichen Geschäftsbetrieb einsetzen.

Die oben genannte Java Technologie setzt so gut wie jeder große Softwarehersteller in irgendeinem seiner Produkte ein, zum Beispiel: VMware, Sophos, Trend Micro, Cisco, Unifi, SAP, und viele weitere mehr.

Ist die Schwachstelle vorhanden und zugänglich, kann sie genutzt werden um uneingeschränkt Code auf dem Zielsystem auszuführen. Das bedeutet, ein Angreifer kann mit dem betroffenen System machen was immer er will. (z.B. die komplette Kundendatenbank kopieren, Patente klauen, Zugangsdaten ausspionieren und in der Folge weitere Systeme im Unternehmen kompromittieren.

Die Sicherheitslücke betrifft nahezu jede heute eingesetzte Software wie ERP Systeme, CRM Systeme, Bankingsoftware, Zeiterfassungssoftware, Buchhaltungs- Lohnabrechnungssoftware, Dokumentenmanagementsoftware, Telefoniesoftware, Videochatsoftware usw.

Die gute Nachricht:

Weltweit sind Sicherheitsteams seit dem 10.12.2021 damit beschäftigt die Sicherheitslücke zu analysieren.

Unsere Techniker informieren sich permanent über die Verfügbarkeit von Patches für die von uns betreuten Systeme und treten proaktiv an unsere Servicevertragskunden heran.

Auf Wunsch überprüfen wir Ihre Systeme auf Verwundbarkeit, spielen verfügbare Sicherheitspatches ein und untersuchen verwundbare Systeme auf eine mögliche Kompromittierung.

ADICOM Consulting GmbH
Ein Unternehmen der ADICOM GROUP
Mauerstraße 47
15749 Mittenwalde

+49 (0) 36 43 - 85 59 4-0
+49 (0) 36 43 - 85 59 4-80
info@adicom-group.de
www.adicom-group.de

Geschäftsführer:
Dipl.-Ing. Peter Schulz
Ing. (FH) Ralf Brummack
AG Cottbus: HRB 9364 CB

Mittelbrandenburgische Sparkasse
IBAN: DE65 1605 0000 3661 0236 31
BIC: WELADED1PMB
USt-IdNr.: DE138545853

Was Sie selbst tun können und müssen:

IBM i Systeme können Sie wie folgt prüfen:

```
qsh
find /qibm/proddata -name log4j-core-2*.jar
find /qibm/userdata -name log4j-core-2*.jar
F6 to spool output
```

Die weiteren Schritte sind dann vom Ergebnis der Prüfung abhängig.

Systemweit kann das Problem durch das Setzen der Umgebungsvariable LOG4J_FORMAT_MSG_NO_LOOKUPS = true umgangen werden:

```
qsh
system -k "ADDENVVAR ENVVAR(LOG4J_FORMAT_MSG_NO_LOOKUPS) VALUE('true') REPLACE(*YES) LEVEL(*SYS)"
CPCA980: Environment variable added.
$
touch -C 37 /QIBM/UserData/Java400/SystemDefault.properties
$
echo "log4j2.formatMsgNoLookups=true" >> /QIBM/UserData/Java400/SystemDefault.properties
$
```

Hier sind (seltene) Effekte auf verwendete Applikationen möglich, welche die entsprechenden Bibliotheken (wofür auch immer) nutzen.

IBM Produkte

IBM stellt ausführliche Informationen für alle IBM Systeme (Hardware und Software) hier bereit:
https://www.ibm.com/blogs/psirt/category/severity-critical/
https://www.ibm.com/blogs/psirt/an-update-on-the-apache-log4j-cve-2021-44228-vulnerability/

Nicht betroffene IBM Produkte sind hier dokumetiert:
https://www.ibm.com/blogs/psirt/an-update-on-the-apache-log4j-cve-2021-44228-vulnerability/#list-of-products

„geheilte“ IBM Produkte
(Für diese Produkte stehen Patches bzw. Workarounds und Handlungsanweisungen bereit)
https://www.ibm.com/blogs/psirt/an-update-on-the-apache-log4j-cve-2021-44228-vulnerability/#Remediated-Products

Anfällige IBM Produkte sind z.B.:

Websphere Applikation Server
https://www.ibm.com/blogs/psirt/?s=websphere+application

und HMC Konsolen Version 9 und 10.
https://www.ibm.com/blogs/psirt/security-bulletin-vulnerability-in-apache-log4j-cve-2021-44228-affects-power-hmc-2/
https://www.ibm.com/support/pages/node/6526172

IBM Spectrum Komponenten
https://www.ibm.com/blogs/psirt/?s=spectrum+44228
IBM Spectrum Protect Client Web GUI und IBM Spectrum Protect for Virtual Environments
IBM Spectrum Protect Operations Center Help system

IBM DB2 Komponenten
https://www.ibm.com/blogs/psirt/?s=db2+44228
IBM® Db2®
IBM® Db2® Warehouse
IBM® Db2® On Openshift and IBM® Db2® and Db2 Warehouse® on Cloud Pak for Data

IBM COGNOS Komponenten
https://www.ibm.com/blogs/psirt/?s=cognos+44228
IBM Cognos Analytics
IBM Cognos Controller

IBM i Access Client Solution (ACS) Versionen 1.1.8.6 und älter sind anfällig für das log4j2 Exploit

integrierten Webserver sind anfällig für das log4j2 Exploit

iNavigator sind anfällig für das log4j2 Exploit
Es wird empfohlen, folgende Fixes zu installieren: IBM i 7.4 – SF99662 level 17
IBM i 7.3 – SF99722 level 36

Weitere Hinweise

Ein Link mit guten Erläuterungen zum Verständnis des bestehenden Problems:
https://logging.apache.org/log4j/2.x/security.html

Sie können über Ihre Softwarehersteller prüfen, ob die Software Log4J nutzt:

1. Öffnen Sie Suchmaschine Google
2. Geben sie den unten genannten CVE Code + den Namen Ihrer Software ein (hier im Beispiel „**SAP**“)

CVE-2021-44228 **SAP**

3. Wenn der Hersteller schon Informationen zu der Lücke bereitstellt, werden Sie auf der Herstellerwebsite etwas dazu finden.
4. Folgen Sie den Informationen und beauftragen/organisieren Sie die Installation von Updates für Ihre Software
5. Sollten Sie keine Informationen finden, probieren Sie das gleiche am Folgetag
6. Haben Sie nach 7 Tagen keine Informationen gefunden, sollten Sie Ihren Systemhersteller per E-Mail kontaktieren und explizit nachfragen ob das Log4J Framework in Ihrer Software zum Einsatz kommt.

Wie immer gilt: Ruhe und einen klaren Kopf bewahren, Augen und Ohren offenhalten und aktuelle Entwicklungen aktiv verfolgen.

Beste Grüße,

Ihr ADICOM® Team