Landespolizeipräsidium · Mainzer Straße 134-146. ·66121 Saarbrücken

Information der
Zentralen Ansprechstelle Cybercrime (ZAC) des Landespolizeipräsidiums Saarland

Landespolizeipräsidium
LPP 2 Kriminalitätsbekämpfung/
Landeskriminalamt

Dezernat LPP 222

Dienst-gebäude: Hellwigstraße 8-10
66121 Saarbrücken

Bearbeiter_in: Schmitt M.O.KHK
Tel.: 0681 962 – 2431
Fax: 0681 962 –2445
E-Mail: cybercrime@polizei.slpol.de

Az: 38/2021

Datum: 11.12.2021

Warnmeldung der zentralen Ansprechstelle Cybercrime (ZAC) Saarland vor KRITISCHER Schwachstelle LOG4j

Log4j ist eine beliebte Protokollierungsbibliothek für Java-Anwendungen. Sie dient der performanten Aggregation von Protokolldaten einer Anwendung.

Von Sicherheitsdienstleistern wird über eine Schwachstelle in log4j in den Versionen 2.0 bis 2.14.1, berichtet, die es Angreifern gegebenenfalls ermöglicht, auf dem Zielsystem eigenen Programmcode auszuführen und so den Server zu kompromittieren.
CVE-2021-44228 [MIT2021]

Die Gefahr besteht dann, wenn log4j verwendet wird, um eine vom Angreifer kontrollierte Zeichenkette wie beispielsweise den HTTP User Agent zu protokollieren.

Ein Proof-of-Concept (PoC) der Schwachstelle wurde auf Github veröffentlicht [GIT2021a] und auf Twitter geteilt [TWI2021]. Neben dem PoC existieren auch Beispiele für Skripte, die Systeme stichprobenartig auf Verwundbarkeit hin untersuchen [GIT2021b]. Skripte solcher Art können zwar Administratoren keine Sicherheit über die Verwundbarkeit geben, aber erlauben Angreifern kurzfristig rudimentäre Scans nach verwundbaren Systemen.

Diese kritische Schwachstelle hat demnach möglicherweise Auswirkungen auf alle aus dem Internet erreichbaren Java-Anwendungen, die mit Hilfe von log4j Teile der Nutzeranfragen protokollieren.

Es sollten die in der BSI Warnmeldung aufgeführten Gegenmaßnahmen unverzüglich getroffen werden.

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

Die Polizei rät:

- Prüfen Sie zeitnah, ob Ihr System betroffen ist.

- Server sollten generell nur solche Verbindungen (insbesondere in das Internet) aufbauen dürfen, die für den Einsatzzweck zwingend notwendig sind. Andere Zugriffe sollten durch entsprechende Kontrollinstanzen wie Paketfilter und Application Layer Gateways unterbunden werden. [BSI2021b]

- Es sollte entsprechend dem Grundschutzbaustein [BSI2021a] ein Update auf die aktuelle Version 2.15.0 [APA2021] (git-tag: 2.15.0-rc2 [GIT2021c]) von log4j in allen Anwendungen sichergestellt werden. Da Updates von Abhängigkeiten in Java-Anwendungen häufig nicht zeitnah erfolgen können, sollte bis dahin die folgende Mitigationsmaßnahme ergriffen werden:

  Die Option "log4j2.formatMsgNoLookups" sollte auf "true" gesetzt werden, indem die Java Virtual Machine mit dem Argument

  "–Dlog4j2.formatMsgNoLookups=True"

  gestartet wird.

  Update 2:

  Alternativ kann auch die Umgebungsvariable LOG4J_FORMAT_MSG_NO_LOOKUPS auf true gesetzt werden. Diese beiden Mitigationsmaßnahmen funktionieren erst ab Log4J Version 2.10.

  Achtung: Diese Maßnahme kann die Funktionsweise der Applikation beeinträchtigen, wenn die Lookup-Funktion tatsächlich verwendet wird.

- *Was Sie tun können, wenn Sie betroffen sind:*

  - Wenn Sie feststellen, dass Ihr System kompromittiert ist, trennen Sie das infizierte System sofort vom Internet.

  - Erstatten sie Strafanzeige bei der Polizei.

Mit freundlichen Grüßen,
i.A.
KHK M.O. Schmitt

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

Quellen:

[LUN2021] - RCE 0-day exploit found in log4j, a popular Java logging package
https://www.lunasec.io/docs/blog/log4j-zero-day/

[TWI2021] - Twitter Beitrag Apache Log4j2 jndi Remote Code Execution (RCE)
https://twitter.com/P0rZ9/status/1468949890571337731

[GIT2021a] - Proof of Concept (PoC) zur CVE-2021-44228
https://github.com/tangxiaofeng7/apache-log4j-poc

[GIT2021b] - Skript zur Überprüfung auf Verwundbarkeit
https://gist.github.com/byt3bl33d3r/46661bc206d323e6770907d259e009b6

[GIT2021c] - Github release von Log4j
https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2

[GIT2021d] Github Diskussion zu Log4j 1.x Betroffenheit
https://github.com/apache/logging-log4j2/pull/608#issuecomment-990494126

[APA2021] - Log4J Updates
https://logging.apache.org/log4j/2.x/download.html[APA2021b] - CVE-2021-44228https://logging.apache.org/log4j/2.x/

[MIT2021] - CVE-2021-44228 in der NVD
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

[BSI2021a] - Grundschutzbaustein OPS.1.1.3
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2021.html

[BSI2021b] - Grundschutzbaustein NET.3.2
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2021.html

[APA2021c] - Apache Kafka Issue
https://issues.apache.org/jira/browse/KAFKA-13534

[BRO2021] - Broadcom/Symantec Security Advisory
https://support.broadcom.com/security-advisory/content/security-advisories/Symantec-Security-Advisory-for-Log4j-2-CVE-2021-44228-Vulnerability/SYMSA19793

[CIS2021] - CISCO Security Advisory

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd

[FSE2021] - F-Secure Service Status
https://status.f-secure.com/incidents/sk8vmr0h34pd

[MCA2021] - McAfee Knowledge Base Artikel
https://kc.mcafee.com/corporate/index?page=content&id=KB95091

[SOP2021] - Sophos Security Advisory
https://www.sophos.com/en-us/security-advisories/sophos-sa-20211210-log4j-rce
CSW # 2021-549032-1232

[TRE2021] - TrendMicro Security Alert
https://success.trendmicro.com/solution/000289940

[UNI2021] - UniFi Network Release Notes
https://community.ui.com/releases/UniFi-Network-Application-6-5-54/d717f241-48bb-4979-8b10-99db36ddabe1

[VMW2021a] - Vmware Response
https://kb.vmware.com/s/article/87068

[VMW2021b] - Vmware Security Advisory
https://www.vmware.com/security/advisories/VMSA-2021-0028.html

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken