SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstelle in log4j veröffentlicht (CVE-2021-44228)

Erhöhung der Warnstufe auf Rot

CSW-Nr. 2021-549032-15M0, Version 1.5, 17.12.2021

IT-Bedrohungslage*: 4 / Rot

Sachverhalt

Update 5:
Auf Grund der sich verändernden Informationslage im Zusammenhang mit Schwachstellen in Log4j, hat das BSI ein Übersichtsdokument (zu Detektion und Reaktion) erstellt, in dem u.a. alle bekannten Detektionsmaßnahmen nochmals zusammengefasst wurden. Dieses Dokument soll die Cybersicherheitswarnung des BSI zu der „Log4Shell" genannten Schwachstelle CVE-2021-44228 [MIT2021] in der Bibliothek Log4j um detailliertere Informationen zur Schwachstelle selbst, möglichen Mitigationsmaßnahmen und Detektionsmöglichkeiten konsolidieren und differenzieren.

Das Übersichtsdokument wird auf Basis neuer Erkenntnisse laufend aktualisiert. Die jeweils aktuelle Version finden Sie auf der Webseite des BSI [BSI2021c].

Diese CSW (2021-549032-1432) wird nach dem Update 1.5 nicht weiter aktualisiert.

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. Diese Gefahr besteht, wenn log4j verwendet wird, um eine vom Angreifer kontrollierte Zeichenkette wie beispielsweise den HTTP User Agent die Felder in einer Webanwendung zu protokollieren.

Ein Proof-of-Concept (PoC) zur Ausnutzung 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.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

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

Update 1:
Der Schwachstelle wurde nach Veröffentlichung des Blog-Posts ein CVSS-Wert von 10.0 zugewiesen.

Erste öffentliche Quellen weisen auf breitflächiges Scannen nach verwundbaren Systemen hin. Das BSI kann derartige Scan-Aktivitäten bestätigen.

Update 2:
Im Gegensatz zur ursprünglichen Einschätzung kann die kritische Schwachstelle ggf. auch auf internen Systemen ausgenutzt werden, sofern diese externe Daten entgegennehmen oder verarbeiten.

Einige Produkthersteller haben bereits öffentlich bzgl. einer möglichen (Nicht-)Betroffenheit ihrer Produkte hingewiesen und teilweise bereits Updates veröffentlicht ([APA2021c], [BRO2021], [CIS2021], [FSE2021], [MCA2021], [SOP2021], [TRE2021], [VMW2021a], [VMW2021b], [UNI2021]). Zu den betroffenen Herstellern gehören **beispielsweise**:

- VMWare
- Apache
- UniFi

- Goverment Side Builder (GSB) (ITZ-Bund ist unterrichtet und arbeitet dran)

Diese Liste ist nicht abschließend und erhebt keinen Anspruch auf Vollständigkeit. Zahlreiche weitere Hersteller prüfen aktuell noch eine Betroffenheit.

Update 3:
Auf Github wurde unter [GIT2021e] eine Liste mit Sicherheitswarnungen für Produkte von über 140 Herstellern veröffentlicht. Einige der Links verweisen direkt auf Herstellerseiten, die neben Informationen zur Verwundbarkeit auch Updates für Ihre Produkte bereitstellen. Die Inhalte wurden durch das BSI stichprobenartig verifiziert und sollen als erste Orientierungshilfe zur Überprüfung der eigenen Verwundbarkeit dienen.

Das NCSC NL (Nationaal Cyber Security Centrum Netherlands) plant im Laufe des Nachmittages die Veröffentlichung eines Github-Repositories unter [NCSC2021] mit gesicherten Informationen zu betroffenen Herstellern.

Update 4:
Inzwischen wurde die Liste mit der Informationssammlung durch NCSC-NL [NCSC2021] veröffentlicht.

Entgegen der anderslautenden ursprünglichen Annahme ist Berichten zufolge die Programmbibliothek auch in den Versionen 1.x verwundbar. In diesen Fällen sei die Verwundbarkeit jedoch nur über eine schadhafte Programmkonfiguration ausnutzbar, sodass eine Ausnutzung weit weniger wahrscheinlich erscheint. [GIT2021d]

Bewertung

Log4j wird in vielen Java-Anwendungen eingesetzt. Der Schutz gegen eine aktive, breite Ausnutzung ist durch die Verfügbarkeit eines PoC sehr gering. Das Patchmanagement von Java-Anwendungen ist nicht trivial, sodass bis zu einer Update-Möglichkeit die kurzfristigen Mitigationen empfohlen werden.

Wenngleich das Nachladen von Schadcode über den im PoC aufgezeigten Weg bei Grundschutz-konform eingerichteten Systemen fehlschlagen sollte, sind auch andere Wege denkbar, ggf. auch automatisiert und ohne Nachladen Schadcode zur Ausführung zu bringen. Hierbei ist die Komplexität im Vergleich zum PoC deutlich erhöht.

Update 1:
Aufgrund der weiten Verbreitung der Bibliothek ist es nur schwer absehbar, welche Produkte alle betroffen sind.

Das BSI sieht aktuell eine Erhöhung der IT-Bedrohungslage für Geschäftsprozesse und Anwendungen. Durch das aktuell breitflächige Scannen ist eine mögliche anschließende Infektion von anfälligen Systemen und Anwendungen, auch auf Grund aktuell oftmals noch fehlenden Patches, nicht auszuschließen.

Update 2:
Das Ausmaß der Bedrohungslage ist aktuell nicht abschließend feststellbar. Die Reaktions- und Detektionsfähigkeit des IT-Betriebes ist kurzfristig geeignet zu erhöhen, um angemessen die Systeme überwachen zu können bzw. zu reagieren.

Aus mehreren CERT-Quellen erreichten das BSI Benachrichtigungen über weltweite Massenscans und versuchte Kompromittierungen. Es gibt bereits erste Meldungen über erfolgreiche Kompromittierungen (bislang u.a. mit Kryptominer).

Es sind zudem Ausnutzungen der Schwachstelle möglich, die kein explizites Nachladen eines Schadcodes benötigen. Dies gefährdet auch Grundschutz-konforme Systeme, die i.d.R. keine Verbindung ins Internet aufbauen können.

Aktuell ist noch nicht bekannt in welchen Produkten diese Bibliothek eingesetzt wird, was dazu führt, dass zum jetzigen Zeitpunkt noch nicht abgeschätzt werden kann, welche Produkte von der Schwachstelle betroffen sind.

Auch interne Systeme, die Informationen oder Daten von anderen Systemen verarbeiten, können ggf. kompromittiert werden und sind daher umgehen zu patchen.

Aufgrund der neuen Sachverhalte hat das BSI entschieden die Warnmeldung von der Warnstufe Orange auf Rot hochzustufen.

Update 3:
Neben erfolgreichen Kompromittierungen mit Kryptominern gibt es unter [3602021] erste Hinweise darauf, dass die Schwachstelle auch von Botnetzen ausgenutzt wird. Die Wahrscheinlichkeit ist groß, dass die mit dieser Schwachstelle in Verbindung stehenden Angreiferaktivitäten in den nächsten Tagen deutlich zunehmen werden.

Update 4:
Zusätzlich zu der Installation von Kryptominern und der Ausnutzung durch Botnetze gibt es auch öffentliche Berichte, die auf das Nachladen von Cobalt Strike-Beacons hinweisen. Cobalt Strike ist eine Pen-Testing-Software, die auch von Angreifern genutzt wird, um Angriffe auf IT-Netzwerke durchzuführen. [MS2021a]

Die Schwachstelle kann nicht nur zum Nachladen von weiterer Schadsoftware genutzt werden, sondern auch für die Offenlegung von vertraulichen Daten (z. B. API-Keys). Hierfür ist kein Nachladen von externer Schadsoftware notwendig, sodass diese Ausnutzung mit einer Anfrage durchgeführt werden kann.

Maßnahmen

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.

Update 2:
Die Log4J Versionen 1.x sind von der aktuellen Schwachstelle nach aktueller Kenntnis nicht betroffen [GIT2021d]. Die Version 1.x wird, auch wenn sie noch in diversen Produkten eingesetzt wird, nicht mehr vom Hersteller unterstützt. Sie

ist End-of-Life und durch andere Schwachstellen verwundbar. Daher sollten auch noch eingesetzte Log4J Versionen 1.x ebenfalls auf eine nicht-verwundbare Version 2.x aktualisiert werden.

Sofern das Log4j als eigene jar-Datei vorliegt, kann diese ggf. ausgetauscht werden. Hier ist vorab die Herstellerdokumentation zu prüfen, ob und unter welchen Umständen dieses Verfahren das System absichert.

Als Alternative, die auch in Versionen ab 2.0-beta9 und höher funktioniert, empfiehlt der Hersteller die Klasse JndiLookup aus dem Klassenpfad zu löschen [APA2021b]:
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

Sofern die Hersteller Updates zur Verfügung stellen, sollten diese umgehend installiert werden.

In den jeweilig zu verantwortenden Bereichen sollte qualifiziertes IT-Personal eingesetzt werden, um die kritischen, vor allem von außen zu erreichende Systeme engmaschig zu überwachen.

Um potentiell betroffene Systeme leichter zu identifizieren, kann zunächst überprüft werden, welche Systeme Java als Installationsvoraussetzung haben oder Java installieren. Zu solchen Systemen sollten die Meldungen des jeweiligen Herstellers prioritär geprüft werden. Sofern seitens des Herstellers noch kein Security Advisory veröffentlicht wurde, sollte eine entsprechende Anfrage gestellt werden.

Da eine Ausnutzung nicht zwingend ein Nachladen von Schadcode aus dem Internet benötigt, sondern bereits mit einer einzigen Anfrage möglich ist, muss für alle verwundbaren Systeme die Angriffsfläche reduziert werden. Konkrete Schritte hierzu sind:

- Nicht zwingend benötigte Systeme abschalten.
- Netzwerke segmentieren, sodass verwundbare Systeme von nicht extern-verbundenen/internen Systemen isoliert werden

Systeme, die aufgrund der Kritikalität für unabdingbare Geschäftsprozesse nicht abgeschaltet werden können:

- In Web-Application-Firewalls (WAF), Intrusion Prevention Systemen (IPS) oder Reverse Proxies Verbindungen, die Angriffsmuster aufweisen, direkt ohne Weitergabe an die Fachapplikation abweisen oder nicht zwingend benötigte HTTP-Header auf statische Werte setzen.
- Blockieren aller nicht zwingend notwendigen, ausgehenden Verbindungen.
- Umfassendes Logging und die Protokollierung aller eingehender und ausgehender Verbindungen, um im Nachgang eine Kompromittierung leichter feststellen zu können.
- Anomaliedetektion auf dem Host betreiben.
- Prüfen, mit welchen Rechten der betroffene Dienst betrieben wird und diese auf das notwendige Minimum reduzieren.
- Verbindungen zu anderen Systemen sollten getrennt werden.

Für nach Bekanntwerden der Schwachstelle gepatchte Systeme muss zusätzlich untersucht werden, ob diese bereits kompromittiert wurden. Dies betrifft auch Systeme, die nicht direkt mit dem Internet verbunden sind, da diese über verbundene Systeme kompromittiert worden sein könnten.

Informieren Sie sich auf den Webseiten der von Ihnen eingesetzten Hersteller (u.a. den oben genannten) über Patches und Workarounds und spielen sie diese unverzüglich ein.

Update 3:
Unter [GIT2021e] und [NCSC2021] wurden Hinweise zu einer möglichen Betroffenheit zahlreicher Produkte veröffentlicht. Als erste Orientierungshilfe ist es zu empfehlen, diese Listen mit eigenen eingesetzten Produkten abzugleichen. Das BSI hat die Inhalte nicht vollständig verifiziert. Die Listen werden mit hoher Wahrscheinlichkeit fortlaufend aktualisiert, so dass eine mehrmalige Überprüfung notwendig ist.
Dieser Abgleich kann die zwingend erforderlichen eigenen Überprüfungsmaßnahmen ergänzen.

Da zum aktuellen Zeitpunkt keine gesicherte Aussage darüber getroffen werden kann, in welchen Produkten die Bibliothek eingesetzt wird, kann das unter [GIT2021h] veröffentlichte Tool zum Suchen von betroffenen log4j Bibliotheken verwendet werden. Das Tool durchsucht dabei Hashsummen-basiert .jar und .war Archive nach eindeutigen Java-Klassen. Da lediglich die offiziell kompilierten Releases erkannt werden, kann es insbesondere bei Linux-Systemen vorkommen, dass betroffene log4j Bibliotheken nicht erkannt werden.

Unter [GIT2021f] wurde eine Auflistung von Befehlen veröffentlicht, mit denen man Log-Daten auf eine mögliche Ausnutzung der Schwachstelle überprüfen kann. Im Falle von Treffern ist es dringend zu empfehlen weitere

Maßnahmen sofort einzuleiten. Zu diesen zählen z.B.: Netztrennung, Suche nach den Schwachstellen, deren Schließung (ggf. durch Neuinstallation) und dann die Feststellung/Bereinigung einer möglichen Kompromittierung mit Schadcode unter Betrachtung auch weiterer benachbarter und dahinter liegender Systeme (lateral movement).

Update 4:
Das alleinige Aktualisieren der Bibliothek über die Softwareverwaltung von Betriebssystemen reicht zur Schließung der Schwachstelle nicht aus. Die Bibliothek wird häufig von Softwareherstellern in die Auslieferungsdateien der eigenen Software direkt integriert und ist daher unabhängig von der auf dem Betriebssystem allgemein installierten Bibliotheksversion. Eine ähnliche Problematik ergibt sich für die verwendete Java-Version.

Der Hersteller des für die Bundesverwaltung über den BSI-Rahmenvertrag verfügbaren Schwachstellenscanners GSM hat eine Scan-Konfiguration zur Verfügung gestellt. In dem Feed mit der Version 202112130808 steht diese Möglichkeit zur Verfügung. Der Schwachstellenscanner ist je nach Version kostenfrei bzw. zu reduzierten Preisen abrufbar. Weitere Informationen finden IT-Sicherheitsbeauftragte der Bundesverwaltung im internen Bereich der BSI-Internetseite.
Bei Betroffenheit (d.h. erfolgreiche Ausnutzung der Schwachstelle, ggf. mit weiteren Aktivitäten durch die Täter) bittet das BSI um Information über die jeweiligen etablierten Meldewege.

Links

[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-2021-44228
https://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

Update 2:

[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
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

[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

Update 3:

[GIT2021e] Security Advisories / Bulletins linked to Log4Shell (CVE-2021-44228)
https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

[3602021] Threat Alert: Log4j Vulnerability Has Been adopted by two Linux Botnets
https://blog.netlab.360.com/threat-alert-log4j-vulnerability-has-been-adopted-by-two-linux-botnets/

[GIT2021f] log4j RCE Exploitation Detection
https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b

[GIT2021g] log4shell-detector
https://github.com/Neo23x0/log4shell-detector

[GIT2021h] Simple local log4j vulnerability scanner
https://github.com/hillu/local-log4j-vuln-scanner

[NCSC2021] Security Advisories linked to Log4Shell (CVE-2021-44228)
https://github.com/NCSC-NL/log4shell

Update 4:

[MS2021a] Guidance for preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation

https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

Update 5:

[BSI2021c] - Log4J Reaktions- und Mitigationsdokument
https://bsi.bund.de/dok/log4j