Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

**SCHWACHSTELLE** | GEFÄHRDUNG | VORFALL | IT-ASSETS

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

*CSW-Nr. 2021-549032-11k2, Version 1.1, 10.12.2021*

IT-Bedrohungslage*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

**TLP:WHITE: Unbegrenzte Weitergabe**

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

## Sachverhalt

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 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.

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

* 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.

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

# 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:**
Auf Grund 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.

# 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.

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

# 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
[APA2021] - Log4J Updates
https://logging.apache.org/log4j/2.x/download.html
[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

# Anlagen

## Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

## Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.