Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

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

# Kritische "Log4Shell" Schwachstelle in weit verbreiteter Protokollierungsbibliothek Log4j (CVE-2021-44228)

*CSW-Nr. 2021-549177-1032, Version 1.0, 14.12.2021*

IT-Bedrohungslage*: 4 / Rot

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

Die sogenannte "Log4Shell" Schwachstelle mit der CVE-2021-44228 [MIT2021] in der weit verbreiteten Log4j Protokollierungsbibliothek für Java-Anwendungen wurde am 10.12.2021 auf dem Blog eines IT-Dienstleisters für IT-Sicherheit veröffentlicht [LUN2021]. Der Schwachstelle wurde nach Veröffentlichung des Blog-Posts ein CVSS-Wert von 10.0 zugewiesen [NVD2021].

Die Protokollierungsbibliothek dient der performanten Aggregation von Protokolldaten einer Anwendung. Die veröffentlichte Schwachstelle ermöglicht es Angreifenden ab den Versionen 2.10 auf dem Zielsystem eigenen Programmcode auszuführen, was zur Kompromittierung des Zielsystems führen kann. Dabei kann die Schwachstelle, durch die Verwendung einer speziellen Zeichenkette, trivial ausgenutzt werden. Die Schwachstelle kann nicht nur zum Nachladen von weiterer Schadsoftware genutzt werden, sondern auch für die Exfiltration von vertraulichen Daten (z. B. Umgebungsvariabeln). Hierfür ist kein Nachladen von externer Schadsoftwarenotwendig, sodass diese Ausnutzung mit einer (einfachen) Anfrage durchgeführt werden kann. Eine ähnliche Schwachstelle ist auch für die nicht mehr im Support befindlichen Versionen

* 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.

1.x gemeldet worden, hierbei scheint die Ausnutzung allerdings komplexer zu sein. Da die Versionen 1.x jedoch den End-of-life (EOL) Status erreicht haben, wird es zu diesen keine Sicherheitsupdates mehr geben [APA2021a].

Auf GitHub wurde ein Proof of Concept (PoC) [GIT2021a] zur Ausnutzung der Schwachstelle veröffentlicht und über den Mikrobloggingdienst Twitter verbreitet [TWI2021]. Neben dem PoC existieren auch Beispiele für Skripte, die Systeme stichprobenartig auf ihre Verwundbarkeit hin untersuchen [GIT2021b].

Öffentliche Quellen weisen darauf hin, dass seit Bekanntwerden der Schwachstelle breitflächige Scans nach verwundbaren Systemen durchgeführt werden [GIT2021d]. Das BSI kann derartige Scan-Aktivitäten bestätigen. Neben erfolgreichen Kompromittierungen mit Kryptominern gibt es erste Hinweise darauf, dass die Schwachstelle auch durch Botnetze ausgenutzt wird [3602021]. Es gibt zudem öffentliche Berichte, die auf das Nachladen von Cobalt Strike hinweisen. Cobalt Strike ist eine Pen-Testing-Software, die auch von Angreifenden genutzt wird, um Angriffe auf IT-Netzwerke durchzuführen [MIC2021].

Ein Sicherheitsforscher stellt auf GitHub eine Liste der als betroffen identifizierten Produktemit Sicherheitswarnungen von über 140 Herstellern bereit [GIT2021c]. Einige der Links verweisen direkt auf Herstellerseiten, die neben Informationen zur Verwundbarkeit auch Workarounds und / oder Updates für ihre Produkte bereitstellen. Diese Liste wurde durch das BSI stichprobenartig verifiziert und kann als erste Orientierungshilfe zur Überprüfung der eigenen Verwundbarkeit dienen.Zu beachten ist jedoch, dass die Liste der betroffenen Hersteller nicht vollständig ist und womöglich weitere Hersteller, die hier nicht genannt sind, betroffen sein könnten.

Zusätzlich hat das NCSC NL (Nationaal Cyber Security Centrum Netherlands) im Laufe des Nachmittags des 13.12.2021 gesicherte Informationen zur Mitigation und Detektion zu betroffenen Herstellern auf einem GitHub-Repository bereitgestellt[NCS2021].

# Bewertung

Log4j wird in vielen Java-Anwendungen eingesetzt. Die Gefahr einer aktiven, breiten Ausnutzung ist durch die Verfügbarkeit eines PoC und die Variation der möglichen schadhaften Zeichenketten als "sehr hoch" zu bewerten. Hinzu kommt, dass das Patchmanagement von Java-Anwendungen nicht trivial ist, sodass bis zu einer Update-Möglichkeit die kurzfristigen Mitigationen dringend empfohlen werden. Aktuell gibt es keine vollständige Liste aller Produkte, die diese Bibliothek in einer verwundbaren Version einsetzen, so dass zum jetzigen Zeitpunkt nicht abgeschätzt werden kann, welche Produkte von der Schwachstelle betroffen sind. Das BSI stuft die aktuelle IT-Bedrohungslage für Geschäftsprozesse und Anwendungen als extrem kritisch ein (Stufe "Rot").

Die Verwundbarkeit von eingebettetenen Systemen kann derzeit nicht pauschal ausgeschlossen werden. Weiterhin ist zum jetzigen Zeitpunkt davon auszugehen, dass auch Produkte, die im Bereich der kritischen Infrastrukturen eingesetzt werden, verwundbar sein können. Erste Hersteller, wie beispielsweise Siemens [SIE2021], Schneider Electric [SIE2021] und Rockwell Automation [RAU2021] haben bereits Sicherheitshinweise zu ihren Produkten veröffentlicht.

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

Durch das breitflächige Scannen ist eine mögliche anschließende Infektion von anfälligen Systemen und Anwendungen, auch auf Grund aktuell oftmals noch fehlender Updates, nicht auszuschließen. Mehrere (CERT-)Quellen bestätigen die Beobachtungen des BSI über weltweite Massenscans und versuchte Kompromittierungen.

# Maßnahmen

Die Reaktions- und Detektionsfähigkeit des IT-Betriebs ist kurzfristig geeignet zu erhöhen, um potentiell betroffene Systeme angemessen überwachen und im Bedarfsfall geeignet reagieren zu können.

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 [BSI2021a].

Entsprechend dem Grundschutzbaustein [BSI2021b] sollte ein Update auf die aktuellste Version 2.16.0 von Log4j in allen Anwendungen sichergestellt werden [APA2021a] [APA2021b].

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.

Die Verwendung von Analyseskripten (wie bspw. [GIT2021b]) kann Administratoren keine umfassende Sicherheit über die Verwundbarkeit geben, erlaubt es aber kurzfristig rudimentäre Scans nach verwundbaren Systemen durchzuführen.

Bei der erfolgreichen Ausnutzung der Schwachstelle, ggf. mit weiteren Aktivitäten durch die Angreifenden, bittet das BSI um Information über die jeweiligen etablierten Meldewege.

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

# Links

[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/

[APA2021a] - Apache Log4j Security Vulnerabilities
https://logging.apache.org/log4j/2.x/security.html

[APA2021b] - Download Apache Log4j 2
https://logging.apache.org/log4j/2.x/download.html

[BSI2021a] - 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

[BSI2021b] - 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

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

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

[GIT2021d] - A fully automated, accurate, and extensive scanner for finding vulnerable log4j hosts
https://github.com/fullhunt/log4j-scan

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

[MIC2021] - 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/

[NCS2021] - Security Advisories linked to Log4Shell (CVE-2021-44228)
https://github.com/NCSC-NL/log4shell

[NVD2021] - National Vulnerability Database CVE-2021-44228

https://nvd.nist.gov/vuln/detail/CVE-2021-44228

[RAU2021] - Rockwell Automation
https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1133605

[SEL2021] - Schneider Electric Security Bulletin
https://download.schneider-electric.com/files?p_Doc_Ref=SESB-2021-347-01

[SIE2021] - Siemens Security Advisory
https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf

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

# 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.