13. Dezember 2021
12:20 Uhr

Zero-Day-Exploit in log4j Auswirkungen auf b-tix und A-va

Was ist passiert?

Am vergangenen Donnerstag, den 09. Dezember 2021, wurde eine kritische Sicherheitslücke in der weit verbreiteten Java-Bibliothek log4j bekannt. Der Exploit ermöglicht die Ausführung von beliebigem Schadcode über das Internet - eine sogenannte Remote Code Execution, kurz RCE - und somit die Kompromittierung der betroffenen Systeme.

Das Bundesministerium für Sicherheit in der Informationstechnik (BSI) stuft laut seiner BSI-Cyber-Sicherheitswarnung (CSW-Nr. 2021-549032-1332, Version 1.3, 12.12.2021) die IT-Bedrohungslage als "4 / Rot" ein: „Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden."

Betroffen seien alle Releases der Bibliothek zwischen der Version 2.0 und der Version 2.14.1.

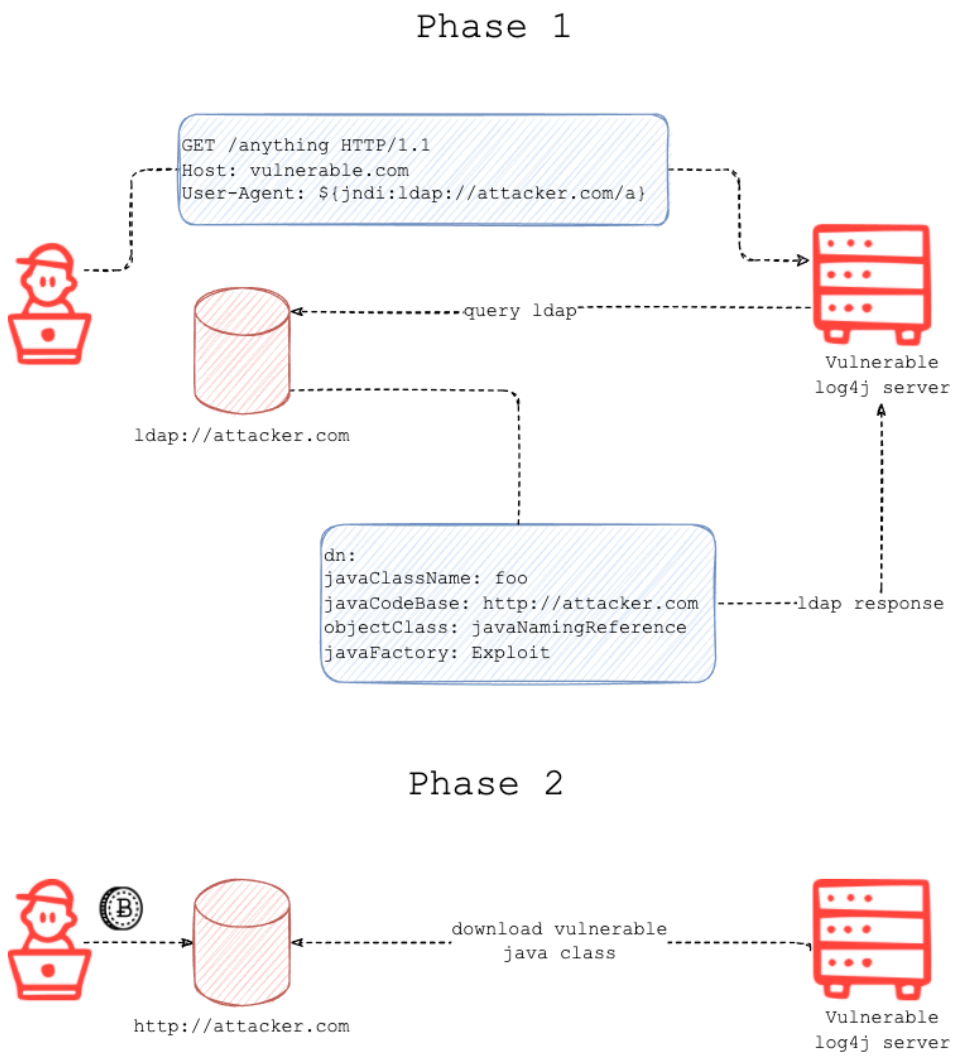
Die Sicherheitslücke in log4j, offiziell bekannt unter der Bezeichnung CVE-2021-44228, ist aus folgenden Gründen als besonders kritisch einzustufen:

- log4j ist eine der am weitesten verbreiteten Bibliotheken für das Logging innerhalb von Java-Anwendungen. Damit sind unzählige Anwendungen und Systeme potenziell gefährdet. Auf GitHub ist inzwischen eine Liste eventuell betroffener Anwendungen verfügbar.
- Die Sicherheitslücke ist einfach auszunutzen und erfordert für den Angriff keinen authentifizierten Zugriff auf das System. Der Angreifer benötigt lediglich die Kontrolle über Strings, welche von log4j geloggt werden.
- Es gibt eine Vielzahl an Angriffsvektoren durch die schiere Anzahl der Operationen, welche insbesondere innerhalb komplexer Systeme geloggt werden.
- Ein Proof of Concept dieses Angriffs ist öffentlich verfügbar. Auf den zugehörigen Link wird an dieser Stelle verzichtet.

Technische Grundlagen des Exploits

log4j bietet seit der Version 2.0, genauer seit der Version 2.0-beta9, die Möglichkeit, JNDI-Lookups bei der Verarbeitung der Logstrings durchzuführen. Diese Funktion ist in den betroffenen log4j-Versionen standardmäßig aktiviert. Logstrings, und damit unmit-

telbar potenzielle Lookups, unterliegen gegebenenfalls der Kontrolle durch den Anwender (in diesem Falle: dem Angreifer) und bieten so die Möglichkeit, schadhaften Code zu injizieren. Ein einfaches Beispiel für einen solchen vom Anwender kontrollierten Logstring ist der HTTP User Agent.



Quelle: Fastly

Welche Gegenmaßnahmen können betroffene Unternehmen ergreifen?

Für alle Anwendungen, welche eine der betroffenen log4j-Versionen einsetzen, empfiehlt sich grundsätzlich ein Update auf die log4j-Version 2.15, welche mittlerweile veröffentlicht wurde. Bestandteil dieser Version ist die standardmäßige Deaktivierung von JNDI-Lookups. Sollte ein kurzfristiges Update der Bibliothek nicht möglich sein, bestehen laut dem US National Institute of Standards and Technology folgende Optionen:

- In log4j-Versionen >2.10 und <=2.14.1 kann der JNDI-Lookup über die system property `log4j2.formatMsgNoLookups` oder die Umgebungsvariable `LOG4J_FORMAT_MSG_NO_LOOKUPS`
- Für Versionen <2.10 wird empfohlen, die Javaklasse `JndiLookup.class` aus dem Classpath zu entfernen, beispielsweise über das Kommando
  `zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class`

Anmerkung: Das NIST trifft hierbei keine explizite Aussage für die Version 2.10.

Zusätzlich wird generell dazu geraten, von einer Kompromittierung der Infrastruktur auszugehen und vorhandene Logdateien auf verdächtige Aktivitäten zu überprüfen. Hierzu wurden auf GitHub einige Kommandos veröffentlicht, welche hierbei unterstützen können.

Was bedeutet das für die Produkte und Services der b-tix GmbH und der A-va GmbH?

Die Antwort auf diese Frage gliedert sich in folgende Dimensionen:

- Welche Auswirkungen hat die Sicherheitslücke auf Produkte und Services, welche von den beiden Gesellschaften hergestellt werden?
- Welche Auswirkungen hat die Sicherheitslücke auf externe Produkte und Services in der Wertschöpfungskette der beiden Gesellschaften?

Eigene Produkte und Services

b-tix und A-va haben die bereitgestellten Angebote sowie deren Infrastruktur vor dem Hintergrund der log4j Sicherheitslücke gründlich analysiert. Aufgrund des eingesetzten Technologiestacks ist der Einsatz von Java-Anwendungen grundsätzlich gering.

Tarifrechner & Snoopr

Die SearchConsole von Snoopr verwendete die log4j Version 2.11.1. Die Anwendung wurde auf die log4j Version 2.15 aktualisiert.

Die ausgelieferte VMware Appliance des Tarifrechners ist **nicht betroffen**, wohl jedoch die Produkte des Herstellers VMware, Inc. selbst. Tarifrechner-Kunden wird deshalb dringend empfohlen, die eigene Virtualisierungsumgebung vor dem Hintergrund des Exploits zu überprüfen.

13. Dezember 2021
12:20 Uhr

b-tix BiPRO Client & easy Client

Die Produkte b-tix BiPRO Client sowie der easy Client setzen log4j in einer Version ein, welche vom Exploit **nicht betroffen** ist.

b-OX & b-OX LD Plattform

Die aktuelle Version der b-OX Plattform ist vom Exploit **nicht betroffen**. Für Kunden, die bereits die neue Version b-**OX** LD einsetzen gelten die Informationen aus den folgenden Abschnitten.

Assets aus der Wertschöpfungskette

b-tix und A-va setzen in ihrer Wertschöpfungskette auf Assets, welche in der Liste potenziell betroffener Software auf GitHub aufgeführt sind. Gemäß der Empfehlung des BSI wurden alle Assets hinsichtlich ihrer Betroffenheit überprüft. Keine der bezogenen Assets setzen mit Stand vom 13. Dezember 2021 eine von der Sicherheitslücke betroffenen Version von log4j ein.

Nichtsdestotrotz werden die b-tix GmbH und die A-va GmbH extern bezogene Assets auf ihre jeweiligen neuesten Versionen aktualisieren, auch wenn sie nicht unmittelbar vom log4j Exploit betroffen waren.

Fazit

Der Exploit in log4j ist insbesondere durch die hohe Verbreitung der Bibliothek in Verbindung mit der vergleichsweise einfachen Möglichkeit zur Ausnutzung von unschätzbarem Ausmaß. Weltweite Massenscans sowie versuchte (und erste erfolgreiche) Kompromittierungen, unter anderem durch Botnets, werden die kommenden Tage noch zunehmen.

Durch das zurückliegende Wochenende sind insbesondere kleine und mittelständische Unternehmen möglicherweise in Verzug und werden die Einleitung von Gegenmaßnahmen nun zu Beginn der Woche nachholen müssen.

Die b-tix GmbH beziehungsweise A-va GmbH konnten durch die umgehende Reaktion auf die Veröffentlichung des Zero-Day-Exploits die notwendigen Maßnahmen am Wochenende bereits weitestgehend abschließen und befinden sich nun in der zusätzlichen Absicherung der Systeme. Auf Basis der Ergebnisse aus der Analyse der eigenen Produkte und Services sowie der Wertschöpfungskette ist aktuell nicht davon auszugehen, dass es zu Ausfällen in der Verfügbarkeit der Services kommen wird.

b-tix GmbH
Lindenstr. 48-52
40233 Düsseldorf

Telefon 0211 / 416 08–400
E-Mail service@b-tix.de
Internet www.b-tix.de

Amtsgericht Düsseldorf, HRB 82497
Geschäftsführer: Markus Heussen
Sitz der Gesellschaft: Düsseldorf