rittmeyer
BRUGG

Schwachstellen in Log4j (auch Log4Shell genannt)

Das deutsche BSI hat die höchste Alarmstufe ausgerufen. Auch das schweizerische Nationale Zentrum für Cybersicherheit (NCSC) nimmt die Situation äusserst ernst und warnt, dass kritische Infrastrukturen angegriffen werden könnten. Die Java-Bibliothek Log4j steckt als Komponente in vielen Java-Anwendungen. Es ist im Moment nicht absehbar, wie viele Internetdienste dabei betroffen sind.

Um was geht es?

Am vergangenen Donnerstag (09.12.2021) wurde bekannt, dass in der vielbenutzten Java-Bibliothek Log4j eine kritische Schwachstelle existiert.
Die Schwachstelle (CVE-2021-44228) wird mit dem Bedrohungsgrad "hoch" eingestuft. Betroffen von der Sicherheitslücke ist Log4j von Version 2.0-beta9 bis 2.14.1. Der Hersteller hat kurzfristig die Version 2.15.0 veröffentlicht, welche die Lücke schliesst.

Es werden vermehrt breit angelegte Scans beobachtet, welche die vorher noch unbekannte Lücke nach verwundbaren Anwendungen absucht. Wenn die Lücke gefunden werden kann, können Hacker diese nutzen, um auf betroffenen Systemen eigene Codes auszuführen und diese komplett zu übernehmen.

Die Schwachstelle, so warnt das NCSC eindringlich, könnte dazu benutzt werden, um kritische Infrastrukturen in der Schweiz anzugreifen. Bisher sind noch keine dahingehenden Berichte eingegangen. Bei den vom NCSC beobachteten Angriffen hätten die Hacker versucht, Malware wie Mirai, Kinsing und Tsunami zu installieren. Kinsing ist ein Cryptominer, die Mirai- und Tsunami-Botnetze werden meistens für DDoS-Attacken verwendet.

Wie ist die Bedrohungslage auf meiner Anlage?

Die verwundbare Java-Bibliothek wird in zahlreichen Java-Anwendungen eingesetzt und ist daher sehr weit verbreitet. Zwar steht für die eigentliche Bibliothek bereits ein Sicherheits-Update bereit, allerdings müssen die darauf basierenden Anwendungen ebenfalls angepasst werden.

Die folgenden Kern-Systeme von Rittmeyer sind nicht betroffen:
- **RITOP**
- **RIFLEX**
- **RISOURCE**
- **RITUNE**
- **RICITY**
- **Rittmeyer Messtechnik**

Weiter sind auch folgende Fremdkomponenten, welche Rittmeyer einsetzt, nicht betroffen
- **Betriebssystem Windows**
- **Firewall SonicWall**
- **VPN Verbindung NetExtender**
- **Westermo**
- **Moxa**
- **Siemens SPS**

Um alles Notwendige zu tun, müssen Organisationen aber zuerst einen Überblick gewinnen, welche die von ihnen verwendeten Systeme und Software-Lösungen Log4j verwenden.

Das NCSC hat bereits aktiv Massnahmen ergriffen. Nachdem der Patch veröffentlicht wurde, wurden sofort die Betreiber von nationaler kritischer Infrastruktur dazu aufgerufen, diesen so schnell wie möglich einzuspielen. Zusätzlich hat man damit begonnen, die Betreiber von über das Internet erreichbaren Log4j-Instanzen direkt zu warnen.

Auch wenn eine bestimmte Lösung im Prinzip verwundbar ist, heisst dies allerdings noch nicht automatisch, dass Angreifer diese tatsächlich ausnützen könnten.

Wie kann ich mich dagegen schützen?

Für die betroffene Java-Bibliothek Log4j gibt es ein Sicherheits-Update.

Sicherheitsspezialisten arbeiten fieberhaft daran, verwundbare Systeme zu identifizieren und Lücken zu schliessen. Das NCSC ruft alle Unternehmen und Organisationen dazu auf, sofort alle Systeme, die mit dem Internet verbunden sind, zu patchen. Für interne Systeme solle man dies danach so schnell wie möglich nachholen.

Systeme, die nicht gepatcht werden können, sollten vom Internet getrennt werden oder zumindest sollte man die von Anbietern empfohlenen Notmassnahmen ergreifen.

Wie kann Rittmeyer Ihnen helfen:

Update Service
Mit dem Update Service übernimmt Rittmeyer das Testen und Installieren der Patches und Hotfix. Besonders für die Firewall und das Betriebssystem wird empfohlen, in regelmässigen Abständen alle verfügbaren Sicherheitsupdates zu installieren, um bekannte Sicherheitslücken zu schliessen.

Schwachstellen Scan
Ein Sicherheits-Spezialist scannt Ihre Anlage mit spezieller Software, um vorhandene Schwachstellen zu erkennen und diese zeitnahe zu schliessen.

Falls Sie sich unsicher fühlen, oder an einer Dienstleistung interessiert sind, wenden Sie sich direkt an Ihren Rittmeyer-Betreuer.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity