Kwetsbaarheid in Log4j-library: alarmerend nieuws voor bouwers van digitale diensten en consumenten

11 januari 2022, 01:00

Tatiana Galibus

Eind december 2021 kwam er alarmerend nieuws voor digitale-dienstenbedrijven over de hele wereld omdat een kritieke kwetsbaarheid in de Apache Log4j-library was ontdekt. Deze opensourcelibrary wordt op grote schaal gebruikt voor het loggen van veiligheids- en prestatie-informatie. Log4j maakt dus frequent deel uit van de diensten en applicaties voor consumenten en bedrijven. Helaas treft het ook productiebedrijven, aangezien het op grote schaal wordt gebruikt in operationele technologieproducten.

Wie wordt erdoor getroffen?

Elke toepassing en dienst die gebruikmaakt van de Java logging library, Apache Log4j (CVE-2021-44228), tussen versie 2.0 en 2.15, waaronder diensten als **Atlassian, Amazon, Microsoft Azure, Cisco, Fortinet, Oracle, Red Hat, Splunk, Soft,** en **VMware**.

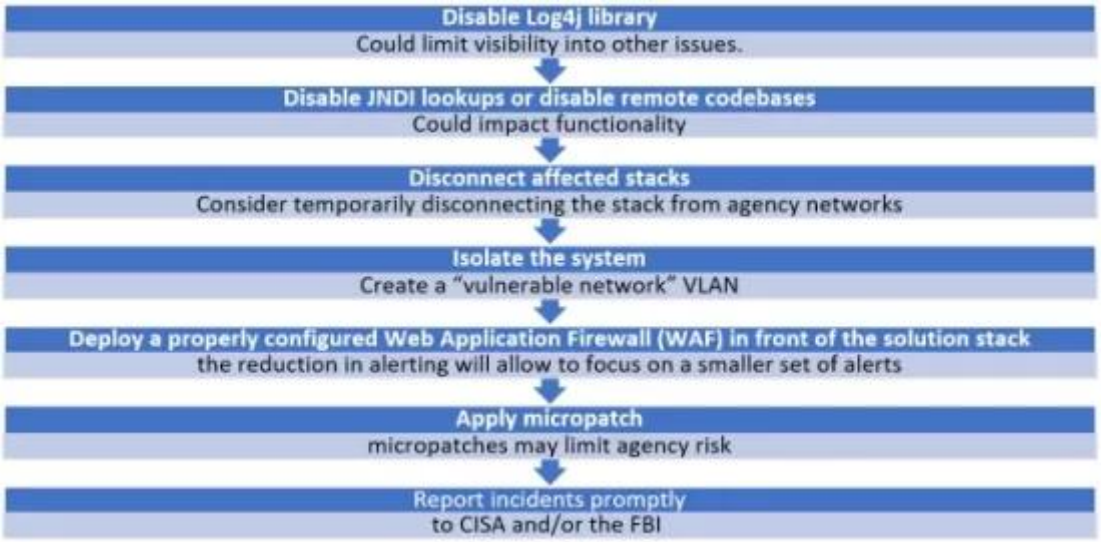
Deze library is dus aanwezig in de meeste populaire apps en websites, en de honderden miljoenen apparaten wereldwijd die de library gebruiken, worden mogelijk blootgesteld aan deze kwetsbaarheid.

Wat is de impact?

Omdat het om een zero-day kwetsbaarheid gaat, kunnen aanvallers via Log4j eender welke code op afstand uitvoeren, over een LAN, WAN of het internet. **Bovendien kan ze in een zeer kort tijdsbestek worden misbruikt**. De kwetsbaarheid treft de **verwerking van logberichten**. Een dreigingsactor kan maken dat het systeem de externe code laadt gewoon door een speciaal daartoe ontworpen bericht te verzenden (uitvoering van commando's op afstand).

Het meest verontrustende met dergelijke aanvallen is dat het voor kleinere bedrijven jaren kan duren om deze kwetsbaarheid te verhelpen, terwijl de hackers van hun kant voortdurend op zoek zijn naar manieren om deze te misbruiken. Het is niet uitgesloten dat ze deze binnenkort zullen gebruiken voor meer gesofisticeerde aanvallen met het oog op meer winst, waardoor ze een tikkende tijdbom kan worden.

Wat is de mitigatie?



Rapporten kunnen hier worden ingediend. Raadpleeg deze pagina om op de hoogte te blijven van de mitigatiemaatregelen.

En nu?

"Ik maak me vooral zorgen over de schooldistricten, de ziekenhuizen en de plaatsen waar slechts één IT'er zich bezighoudt met de veiligheid en geen tijd, budget of tooling heeft voor de beveiliging", aldus Katie Nickels, Director of Intelligence bij Red Canary, gespecialiseerd in cyberveiligheid. *"Over deze organisaties maak ik me de meeste zorgen, kleine organisaties met kleine beveiligingsbudgetten."*

Jammer genoeg zijn voor de aanpak van dergelijke kwetsbaarheden in de toeleveringsketen vaak veiligheidsanalyses door derden en vaardigheden op het gebied van incidentdetectie nodig. Hoe brengt u de problematiek effectief onder de aandacht en hoe gaat u het beste om met Log4j of andere kritieke kwetsbaarheden in de software die u dagelijks gebruikt? De beste oplossing is leren hoe u uzelf kunt beschermen en slim kunt reageren! Sirris en Agoria kunnen u hierbij helpen: in een reeks masterclasses komt u op een toegepaste pragmatische manier alles te weten over cyberveiligheid! Alle opleidingen worden gesubsidieerd door VLAIO, zodat Vlaamse bedrijven slechts 30 procent betalen.

Auteurs



Tatiana Galibus