NFIR Threat Intelligence Report

(Update 3)

Indicaties dat kwetsbaarheid in 'log4j' bibliotheek (CVE-2021-44228) mogelijk actief misbruikt wordt

Datum: 29/12/2021

Versie: 1.3

Beschrijving

Log4j wordt door veel applicaties gebruikt om applicatielogs bij te houden. Recentelijk is een kwetsbaarheid bekend geworden in de Java-bibliotheek 'log4j', waardoor een aanvaller mogelijk in staat is om code uit te voeren binnen de applicatie en/of het systeem waarop log4j ingezet wordt. De kwetsbaarheid ontstaat door een functionaliteit binnen de log4j-bibliotheek welke gebruikt wordt voor het formatteren van logberichten.

Door de manier waarop deze functionaliteit werkt, kunnen er onbedoeld functies aangeroepen worden welke acties kunnen uitvoeren (zoals het downloaden- en uitvoeren van code vanaf een externe server).

De kwetsbaarheid in deze functionaliteit kan worden uitgebuit als er een logbericht weggeschreven wordt. Dit komt in allerlei verschillende situaties voor en is context-afhankelijk, zoals bijvoorbeeld:

- Bij het invullen van een loginscherm waarbij het gebruikersnaam-veld in het logbericht opgenomen wordt;
- Bij het versturen van een verzoek naar een webserver (waarbij een User-Agent-header naar de server verstuurd wordt; dit is een waarde waar een aanvaller controle over kan hebben);
- Bij het aanpassen van elk ander veld in een applicatie waarbij het veld in het logbericht opgenomen wordt.

Kortom: Applicaties die op afstand toegankelijk zijn, gebruikersinvoer kunnen verwerken en log4j (een versie lager dan 2.17.1) gebruiken om deze invoer te loggen, zijn mogelijk kwetsbaar.

Mogelijke Impact

Als een aanvaller in staat is om de kwetsbaarheid succesvol uit te buiten dan kan deze door de aanvaller gecontroleerde code uitvoeren. Dit kan mogelijk resulteren in dat de server waarop de applicatie draait gecompromitteerd raakt. Deze aanval kan uitgevoerd worden vanaf het internet waarbij geen authenticatie vereist is.

Vanuit een gecompromitteerde server kan een aanvaller mogelijk toegang verkrijgen tot de rest van het netwerk. Om deze reden is de impact van de kwetsbaarheid geclassificeerd als **kritiek**.

Indicaties misbruik

Op het moment van schrijven zijn er meerdere indicatoren dat er actief geprobeerd wordt om misbruik te maken van de kwetsbaarheid – waaronder pogingen tot het uitbuiten van de kwetsbaarheid door bekende malafide IP-adressen (https://www.greynoise.io/viz/query/?gnql=cve%3ACVE-2021-44228).

Daarnaast zijn er inmiddels casussen bekend waarbij geprobeerd wordt om crypto coin-miners te plaatsen nadat een systeem via de kwetsbaarheid gecompromitteerd is.

Detectie

Doordat de kwetsbare functionaliteit zich in een populaire Java-bibliotheek bevindt, is de huidige scope of impact niet inzichtelijk. De eerste berichten wijzen er echter wel op dat veelgebruikte webdiensten en softwarepakketten (zoals bijvoorbeeld VMWare vCenter, Apache Solr, ElasticSearch, IBM QRadar SIEM, Palo Alto Panorama, Pulse Secure en UniFi) kwetsbaar lijken te zijn (https://github.com/YfryTchsGD/Log4jAttackSurface). Het is zeer waarschijnlijk dat er veel meer applicaties kwetsbaar zijn welke op het moment van schrijven nog niet bekend zijn. Bovenstaande maakt dat het volledig detecteren van elke vorm van misbruik van de kwetsbaarheid, op het moment van schrijven, complex is.

Aanbeveling

Voor ontwikkelaars van applicaties die gebruik maken van log4j, geldt het volgende advies:
Er is een nieuwe versie van log4j beschikbaar welke te downloaden via de URL **Het advies is om tenminste te updaten naar versie 2.17.1**; https://logging.apache.org/log4j/2.x/download.html. NFIR adviseert om zo snel als mogelijk een upgrade[1] uit te voeren en deze vervolgens uit te rollen naar de betrokken systemen en applicaties.

Op het moment dat upgraden niet mogelijk is, kan de volgende workaround toegepast worden:

1. Een tijdelijke workaround kan worden toegepast door de kwetsbare classes te verwijderen:

```
zip -q -d log4j-core-*.jar
org/apache/logging/log4j/core/lookup/JndiLookup.class
```

Voor applicaties van derden die u gebruikt, adviseert NFIR u om contact op te nemen met de leverancier voor eventuele updates.

Actieplan

Het is belangrijk voor uw organisatie om tenminste de volgende stappen te nemen:

1. Breng in kaart welke individuele leveranciers u heeft voor on-premise softwarepakketten, Software-as-a-Service (SaaS) of andere applicatie-leveranciers;
2. Raadpleeg de website van uw leveranciers en stel vast of er een vorm van 'dependency-lijsten' beschikbaar zijn waarbinnen u kunt controleren of 'log4j' gebruikt wordt binnen de applicatie;
3. Neem contact op met uw leveranciers om te verifiëren of er binnen de applicaties 'log4j' gebruikt wordt en welke versie van log4j er gebruikt wordt;
4. Bereid uw organisatie voor op de situatie dat er onverwacht patches uitgevoerd dienen te worden (buiten de reguliere update-timeframes) en pas patches gecontroleerd toe volgens de voor uw organisatie gebruikelijke procedure.

Heeft u systemen waarvan het risico groot is (bijvoorbeeld systemen met gevoelige of bijzonder persoonsgegevens)? Zo ja heeft u mogelijk indicaties dat Java met log4j gebruikt wordt en zijn er nog geen updates beschikbaar? Overweeg dan om het systeem tijdelijk uit te schakelen.

Wat moet uw organisatie doen bij mogelijk misbruik?

Als uw organisatie vermoedelijk het slachtoffer is geworden van een aanval, is het dringende advies om onderzoek uit te laten voeren naar de toedracht, in hoeverre aanvallers mogelijk andere systemen hebben gecompromitteerd en welke informatie mogelijk ongeautoriseerd geraadpleegd is.

1. Koppel indien mogelijk de getroffen systemen los van het netwerk, maar laat deze aanstaan (in verband met eventuele sporen zoals het vluchtige geheugen – RAM);
2. Laat de getroffen systemen forensisch onderzoeken; zorg voor adequate back-ups;
3. Reset uw wachtwoorden en gebruikersgegevens;
4. Doe aangifte bij de Politie;
5. Overweeg een melding te doen bij de Autoriteit Persoonsgegevens.

Heeft uw organisatie op dit moment een incident? Onze Computer Emergency Response Teams (CERT) staan 24/7 voor organisaties klaar om te ondersteunen bij IT- Security Incidenten.

Bel dan 088 133 0700 en wij doen ons uiterste best om u zo snel mogelijk te helpen. (Meer informatie over onze Incident Response Dienst.)

Over NFIR

NFIR is een specialist in cyberbeveiliging. Bij NFIR zijn cyber-engineers in dienst: Hackers die weten wat ze doen, testers die de werking van ICT-infrastructuren en software begrijpen, privédetectives die, indien nodig, onderzoeken kunnen uitvoeren en adviseurs/consultants die u het juiste advies kunnen geven of die u kunnen ondersteunen bij een incident.

Gespecialiseerd in

- Het verzamelen, identificeren en valideren van digitale informatie
- Onderzoek naar computers, servers, e-mailverkeer, gegevensdragers, websites en personen

Multidisciplinair onderzoek

- Sporen en gegevens verzamelen en reconstrueren
- Heldere rapportage bruikbaar voor juridische procedures en andere officiële instanties

Samenwerking met

- Tactisch rechercheurs, privacy juristen, gerechtsdeurwaarders, Politie, NCSC, IBD, het Openbaar Ministerie en internationale diensten.

NFIR als adviseur Forensisch Onderzoek

- Samen met de opdrachtgever wordt de scope van het onderzoek bepaald
- Praktisch toepasbare adviezen na afronding van het onderzoek

NFIR B.V.
Verlengde Tolweg 2
2517 JV Den Haag
Telefoon: 088 - 323 02 05
info@nfir.nl
https://www.nfir.nl