Rotterdam Port Cyber Resilience

contact@ferm-rotterdam.nl

Aan:

Datum:

Referentie: Log4J

Onderwerp: Informatie en preventie

Afgelopen weekend is bekend geworden dat een veelgebruikt stukje software een ernstige kwetsbaarheid bevat, waardoor veel organisaties kans lopen om gehackt te worden. Het gaat om software met de naam Apache Log4j.

Wij weten echter niet (zeker) of we op dit moment gevaar lopen. We weten wel dat misbruik relatief gemakkelijk is en dat kwaadwillenden actief op zoek zijn naar organisaties om bijvoorbeeld ransomware te installeren.

Om deze reden zouden we graag schriftelijk de bevestiging ontvangen dat deze bekende kwetsbaarheid ons niet kan beschadigen omdat dat de software niet gebruikt wordt in onze systemen, of omdat dat de oplossing al geïmplementeerd is.

We hebben geleerd dat:

- Northwave tooling beschikbaar heeft gesteld om te controleren of Log4J aanwezig is. Deze staat hier: https://github.com/NorthwaveSecurity/log4jcheck.
- Log4j versie 2.15.0 kan nog steeds kwetsbaar zijn. Advies is updaten naar 2.16.0

Voor meer achtergrondinformatie verwijzen we graag naar het NCSC: https://www.ncsc.nl/actueel/nieuws/2021/december/13/log4j-kwetsbaarheid-bereid-u-voor-op-misbruik

Deze kwetsbaarheid wordt gezien als een “tikkende bom”. Vandaar dat we verzoeken graag zo spoedig mogelijk bovenstaande bevestiging te geven. Deze bevestiging graag sturen naar het e-mailadres via welke deze brief is gekomen. Daarnaast zouden we graag advies willen over onze back- up systemen en wat te doen als er wel sprake van misbruik is.

Vriendelijke groet,