MEMORANDUM

PROVINCIE :: UTRECHT

2022BEM37

DATUM	17-1-2022
AAN	Provinciale Staten
VAN	Robert Strijk
ONDERWERP	Java kwetsbaarheid log4j – Update januari 2022

Inleiding
Eind december hebben wij u geïnformeerd over de situatie rondom de kwetsbaarheid in Java software. Met dit memo willen wij u een update geven en informeren over de laatste stand van zaken.

Achtergrond
Vanaf eind november 2022 is een kritische kwetsbaarheid aangetroffen in Apache Log4j 2, een Java logging library. Log4j is een veel gebruikte open source bibliotheek die vooral door IT-ontwikkelaars wordt gebruikt om onder andere vast te leggen of er problemen in een applicatie voorkomen en andere vormen van monitoring/analyse.

Door het misbruiken van de kwetsbaarheid is het voor kwaadwillenden mogelijk om door middel van het uitvoeren van code, controle te krijgen over de server waarop Log4j draait. Log4j wordt door veel organisaties gebruikt voor onder andere clouddiensten, websites en Enterprise-applicaties.

Om deze potentiële crisis te managen is er vanuit het CIBO een (tijdelijk) interprovinciaal Crisis Incident Response Team (CERT-PROV) ingericht waarbij nu alle provincies en BIJ12 actief zijn betrokken. Het belangrijkste doel van dit CERT is het uitwisselen van kennis en het coördineren van gezamenlijke acties, om zo te komen tot een effectieve en geharmoniseerde aanpak.
Binnen de provincie Utrecht is het provinciale CERT opgestart en het Cyberincident Responsplan in werking gesteld. Hierbij hebben wij ons geconformeerd aan de richtlijnen en uitgangspunten van het NCSC voor deze situatie.

Situatie provincie Utrecht
De generieke kantoorautomatisering voorzieningen zijn zo snel mogelijk veilig bevonden door het gebruik van een goede “Acces Manager”.

In de organisatie zijn daarnaast veel specifieke applicaties en systemen in gebruik. Deze zijn, inclusief de bijbehorende externe leveranciers, geïnventariseerd. Dit wordt gedaan om meer duidelijkheid te krijgen over wat zij in werking hebben gesteld om deze kwetsbaarheid te pareren en in hoeverre het gebruik van de betreffende software veilig is. Dit vraagt nog steeds aandacht en er kan nog niet worden uitgesloten dat er op termijn alsnog misbruik gebruik gemaakt wordt van de kwetsbaarheden in Log4J.

Tot op heden zijn geen aanwijzingen aangetroffen van inbraak bij onze systemen of misbruik van onze gegevens. Wel constateren wij dat hier pogingen toe worden ondernomen. Dit legitimeert de ‘verhoogde dijkbewaking’ die sinds december is ingesteld en voorlopig nog wordt gecontinueerd.

Middels zogenaamde immuttable back-ups worden de provinciale gegevens frequent veiliggesteld. Op dit moment is er geen aanleiding om, al dan niet preventief, systemen uit te schakelen die door de provinciale organisatie worden gebruikt.

De interprovinciale CISO’s hebben inmiddels gezamenlijk besloten om het tijdelijke interprovinciale CERT af te schalen. Het dagelijks bijeenkomen is gezien de huidige situatie op dit moment niet langer noodzakelijk, sinds 1

januari wordt er rondom dit issue uitsluitend nog digitaal kennis uitgewisseld. Het CERT kan snel worden opgeschaald als de situatie daarom vraagt.
Het interprovinciale CERT was een goede testcase voor de plannen voor de inrichting van een Interprovinciaal KnoopPunt (IKP) rondom informatiebeveiliging. De samenwerking was prettig en constructief en biedt een goed perspectief op de toekomst.

Vervolg
Het provinciale CERT blijft de komende periode twee keer per week bijeenkomen om de zaken te monitoren en de leerpunten uit deze situatie op te pakken.

Wij werken er hard aan de kans op misbruik en digitale inbreuk zo veel als mogelijk te beperken. We houden u op de hoogte als er belangrijke ontwikkelingen zijn.