MEMORANDUM

PROVINCIE :: UTRECHT

2022BEM20

DATUM	21-12-2021
AAN	Provinciale Staten
VAN	Robert Strijk
ONDERWERP	Actuele situatie rondom Java kwetsbaarheid log4j

Inleiding
Met dit memo willen wij u informeren over de actuele situatie rondom de kwetsbaarheid in Java software, die wereldwijd tot grote zorgen leidt.

Zoals de meesten van jullie ongetwijfeld via de media mee hebben gekregen is vanaf 10 december jongstleden een kritische kwetsbaarheid aangetroffen in Apache Log4j 2, een Java logging library. De kwetsbaarheid wordt in beveiligingsadvies van het Nationaal Cyber Security Center (NCSC) als '*high/high'* ingeschaald.

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.

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-apps.

Interprovinciaal is afgelopen weekend een gezamenlijk communicatiebericht opgesteld. Dit bericht is hieronder integraal opgenomen:

Kwetsbaarheid in Java software - Wat is er aan de hand?
Op 10 december is er in het nieuws gekomen dat een software component "log4j" een kwetsbaarheid zou bevatten. Deze kwetsbaarheid geeft een aanvaller de mogelijkheid om relatief eenvoudig een systeem dat bereikbaar is vanaf het internet volledig over te nemen. Dit component is verwerkt in duizenden software producten, waarvan soms ook de leverancier zich niet bewust is dat het bewuste component in zijn product aanwezig is.

Bij een "normaal" beveiligingsincident is de reikwijdte vaak relatief beperkt, er is bijvoorbeeld één achterdeur die met spoed moet worden dichtgezet. Wat deze situatie bijzonder maakt is dat er per organisatie tientallen achterdeuren open kunnen staan. Hier komt bij dat ook de onderzoekers in de afgelopen dagen nieuwe methoden hebben gevonden om hier misbruik van te maken. Een technische inrichting die op maandag nog als veilig werd beschreven geldt nu als een hoog risico situatie. Een passende analogie is dat we hier niet spreken over vlam in de pan maar van een complete bosbrand waarbij de wind telkens van richting lijkt te veranderen. Duizenden ICT'ers zijn daarom sinds vrijdag 10 december in de weer om systemen met spoed te voorzien van bijgewerkte software, of ze onbereikbaar te maken indien deze updates nog niet beschikbaar zijn.

Het Nationaal Cyber Security Centrum maakte eerder deze week bekend dat zij hebben geconstateerd dat er in ieder geval op 1 december ook al sprake is geweest van inbraken op basis van deze achterdeur. Dit zou betekenen dat je als organisatie, ook als je op 10 december direct hebt ingegrepen, mogelijk toch al gecompromitteerd bent. Daarom is er een advies uitgegaan om in ieder geval een backup van alle gegevens veilig te stellen van, voor 1 december, om daar eventueel op terug te kunnen vallen. Deze reservekopie moet offline worden opgeslagen zodat een indringer hier geen grip op kan krijgen.

Daarnaast adviseert het NCSC om "verhoogde dijkbewaking" in te stellen. In feite gaat het om extra capaciteit (mensen en middelen) om systemen en ICT infrastructuur nauwlettend in de gaten te houden op signalen van inbraak. Inmiddels hebben alle aangesloten provincies aangegeven dit ingericht te hebben.

Provincies die niet op de juiste manier reageren op deze situatie, kunnen geconfronteerd worden met mogelijke gegevens diefstal, het gijzelen van systemen of ongeautoriseerde toegang tot systemen die invloed hebben op de

fysieke veiligheid zoals bruggen, sluizen en verkeersregelinstallaties. Om deze reden is er een (tijdelijk) interprovinciaal Crisis Emergency Response Team (CERT) ingericht waarbij de provincies zijn aangesloten. Dit CERT-Provincies bestaat uit de CISO's en specialisten. Het belangrijkste doel van dit CERT-Provincies is het uitwisselen van kennis en het coördineren van gezamenlijke acties, om zo te komen tot een effectieve en geharmoniseerde aanpak.
Vanuit het CERT-Provincies zal er op regelmatige basis gecommuniceerd worden over de voortgang van deze situatie. Mochten er naar aanleiding van dit bericht vragen ontstaan dan verwijzen wij u graag naar het deelnemende lid (CISO) CERT-Provincies, binnen uw organisatie.

Voor meer achtergrond informatie verwijzen wij u ook graag naar onderstaand artikel in Binnenlands bestuur:

https://www.binnenlandsbestuur.nl/digitaal/nieuws/nu-pas-begint-het-log4j-securitydrama.19290415.lynkx

Situatie provincie Utrecht
Om de impact van deze kwetsbaarheid voor onze eigen organisatie zoveel als mogelijk te beperken is een aantal acties in gang gezet. Het provinciale CERT is geactiveerd, net als het recentelijk vastgestelde Cyberincident Responsplan. De CISO van de provincie neemt ook dagelijks deel aan het interprovinciale CERT met alle andere provincies.

Uit de eerste analyses is naar voren gekomen dat de interne systemen en de generieke kantoorautomatisering van de provinciale organisatie relatief veilig zijn door een goede Acces Manager.
Mogelijke kwetsbaarheden zitten vooral bij de diverse specifieke ICT-dienstenleveranciers en de applicaties die wij gebruiken in de verschillende domeinen van de organisatie. Het applicatiebeheer hiervan is decentraal belegd. Dit wordt nu geïnventariseerd en er wordt met de diverse leveranciers contact gelegd om meer duidelijkheid te krijgen over wat zijn hebben gedaan om deze kwetsbaarheid te pareren en in hoeverre het gebruik van de betreffende software veilig is.

Daarnaast is een back-up van voor 1 december veilig gesteld. Op dit moment is er geen aanleiding om, al dan niet preventief, systemen uit te schakelen die door de provinciale organisatie worden gebruikt.

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.