

Kennisgeving aan de gemeenteraad

Documentnummer: 201542024

Zaaknummer: Z/21/088692

Portefeuillehouder(s): burgemeester

Voor vragen

Naam: Piet Hoogstraten, adviseur informatiebeveiliging
Telefoon: 06-11795494
E-mail: p.hoogstraten@1stroom.nl

Komt niet terug tot besluitvorming in de raad

Onderwerp: Kwetsbaarheden in Log4j applicaties

Aanleiding voor deze kennisgeving

De IBD (Informatie Beveiligingsdienst Gemeenten) heeft ons gewaarschuwd voor het feit dat er een ernstige kwetsbaarheid is aangetroffen in een veelgebruikt stukje software voor logging – de JAVA-tool log4j, een bouwsteen voor software.

Log4j kan bij wijze van spreken voorkomen in elke webapplicatie met een invulveld (inloggen, formulieren, keuzevelden etc.). Ernstig betekent in deze context: een hoge kans op misbruik met een grote schade. Misbruik van de kwetsbaarheid maakt het mogelijk om het betreffende systeem op afstand te misbruiken. Bijvoorbeeld de installatie van ransomware.

Relevant beleidskader

Informatiebeveiliging en privacybescherming

Inhoud van mededeling

Bijna wekelijks worden wij door de IBD geïnformeerd over kwetsbaarheden in systemen en software. Waarom is in dit specifieke geval dan sprake van een ernstig probleem?

Wijd verspreid: log4j is onderdeel van zo veel verschillende applicaties en apparaten dat de Informatie Beveiligingsdienst van de VNG (IBD) inschat dat iedere gemeente hier mee te maken heeft.

Moeilijk te detecteren: Het is voor een organisatie lastig om erachter te komen waar log4j een rol in speelt.

Soms gebruikt in kritieke systemen: log4j is onderdeel van systemen voor thuiswerken en applicaties voor primaire processen.

Moeilijk (zelf) te verhelpen: Omdat het gaat om een bouwsteen binnen software en systemen is een organisatie niet altijd zelf in staat om die te verhelpen.

De kwetsbaarheid kan resulteren in een aanval met gijzelsoftware: Kwaadaardige software waarbij onze organisatie wordt afgeperst, nadat het digitale systeem of de bestanden erop met een code op slot zijn gezet. De aanvaller biedt de code tegen betaling aan, zodat de bestanden weer benaderd kunnen worden. Maar dit is niet zeker.

Welke acties en maatregelen zijn inmiddels ondernomen?

Onze ICT-partner, de RID, onderzoekt welke producten en applicaties gebruik maken van dit stukje software. Daar waar mogelijk en beschikbaar worden de patches¹ zo spoedig mogelijk geïnstalleerd. De firewall is inmiddels aangepast, zodat ongewenst verkeer zoveel mogelijk wordt geblokkeerd. Echter, absolute zekerheid kan helaas niet worden gegarandeerd. De gemeentelijke websites zijn op basis van de informatie van de IBD gecontroleerd (gescand) en de hierboven genoemd kwetsbaarheid is niet aangetroffen). Bij de RID is een taskforce ingesteld, die belast is met de inventarisatie van alle hard- en software, de mogelijke aanwezigheid van Log4J en de coördinatie van de herstelwerkzaamheden. Tot slot zijn alle medewerkers van 1Stroom door middel van een bericht op Binnenshuis geïnformeerd met het verzoek om verdachte situaties direct te melden bij de RID.

Tot slot

De softwareleveranciers zullen de komende dagen/weken patches uitleveren die de kwetsbaarheid moeten mitigeren. Uiteraard dienen deze updates zo spoedig mogelijk geïnstalleerd te worden. Dit om de mogelijke risico's zo snel mogelijk in te dammen. Daardoor is het mogelijk dat applicaties en systemen tijdelijk niet beschikbaar zijn. We proberen natuurlijk de gevolgen voor de dienstverlening zoveel mogelijk te beperken, maar enig ongemak is niet te voorkomen.

Westervoort, 15 december 2021.

Burgemeester en wethouders van Westervoort

M. Sluiter MA
secretaris

drs. A.J. van Hout
burgemeester

¹ Een patch is een nieuwe versie van de software, waarmee de leverancier de kwetsbaarheid dus hersteld. Er worden verder geen nieuwe functies toegevoegd.