Kwetsbaarheden in Log4j
Lessen voor gemeenten en de IBD

Op 10 december ontving de IBD informatie over ernstige kwetsbaarheden[1] in de java-bibliotheek Log4j (Log4shell), een veelgebruikte bouwsteen voor het loggen van gebeurtenissen in hard- en software.[2] Voor deze kwetsbaarheid was een exploit gepubliceerd: een mogelijkheid om misbruik te maken. In dit document kijken we terug op de eerste fase van de incident respons en duiden we de betekenis voor gemeenten. Dit document is mede tot stand gekomen op basis van gesprekken met en een review van CISO's van gemeenten en leveranciers.

Kwetsbaarheid in een bouwsteen

Log4shell had een hoge kans op misbruik en een hoge impact. Ernstige (of hoog/hoog) kwetsbaarheden zien we vaker, zo'n 20 tot 30 keer per jaar.[3] Wanneer zoiets voorkomt in systeemsoftware, netwerkcomponenten of virtualisatiesoftware dan is het alle hens aan dek. Een dergelijke kwetsbaarheid in een zo veel gebruikte bouwsteen van software is zeldzaam en zagen we hooguit eerder in 2014 toen er een kwetsbaarheid in OpenSSL[4] gevonden is. Log4j blijkt te worden gebruikt in tienduizenden softwarepakketten.

Betekenis voor gemeenten

Configuratiemanagement

Pas wanneer je weet wat je in huis hebt, is het mogelijk om dit actueel te houden. Het bijhouden van het actuele overzicht van hard- en software ofwel configuratiemanagement is een basisvoorwaarde voor een veilige informatiehuishouding. Gemeenten dienden in het geval van de Log4j-kwetsbaarheden daarnaast nog vast te stellen waar een specifieke java-bibliotheek voorkomt in de in gebruik zijnde softwarepakketten. Geen sinecure, omdat bij de gebruiker van software vaak niet bekend is uit welke onderdelen software is opgebouwd.

Stand van zaken bij leveranciers[5]

Voor zicht op het gebruik van Log4j was daarom medewerking van softwareleveranciers nodig. Gemeenten dienden erop toe te zien dat de risico's rond de kwetsbaarheden beheerst waren. Leveranciers werkten in het algemeen goed mee aan het tijdig oplossen van de kwetsbaarheden. In enkele gevallen liet de oplossing van leveranciers op zich wachten of was onduidelijk of een oplossing afdoende was. Daar waar gemeenten zelf niet of onvoldoende contact kregen met leveranciers is gebruik gemaakt van de kracht van het collectief.[6]

Risicomanagement en prioritering

Log4shell bleek aanwezig in veel verschillende softwarepakketten. Het is van belang dat een organisatie de grootste risico's eerst aanpakt als het nodig is om keuzes te maken.

(Voorbereiden) Incidentmanagement

De risico's van de kwetsbaarheid waren zo hoog dat gemeenten zich dienden voor te bereiden op misbruik. Er zijn vooralsnog[7] geen noemenswaardige incidenten geweest bij Nederlandse gemeenten waardoor de voorbereidingen op het incidentmanagement gezien kunnen worden als een realistische oefening. Daarbij is voor zover de IBD kan vaststellen vooral beproefd dat de diverse betrokkenen elkaar konden vinden en elkaar op de hoogte hielden van de stand van zaken.[8]

Collectieve aanpak

Als collectieve voorziening van Nederlandse gemeenten zorgde de IBD voor de zogeheten situational awareness (wat is er aan de hand, hoe erg is dat en wat zijn de ontwikkelingen). De IBD informeerde met dagelijkse updates de contactpersonen van gemeenten over de stand van zaken en het bijbehorende handelingsperspectief.
Om de juiste keuzes te kunnen maken publiceerde de IBD een afwegingskader.[9] Dit afwegingskader was bedoeld voor de omgang met systemen waarbij de kwetsbaarheid nog niet was opgelost of waar dat onduidelijk was. De IBD vertegenwoordigde gemeenten in de overleggen van het Nationaal Crisis Centrum (NCC), onderdeel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC). De informatie uit deze overleggen is gedeeld met de doelgroep. Omdat het ook informatie betrof voor bestuurders en managers stuurde de IBD ook een bericht aan de gemeentesecretarissen (via de kringen van de Vereniging van Gemeentesecretarissen) en bestuurders (via de VNG Commissie Informatiesamenleving).[10] De IBD zocht contact met de softwareleveranciers van gemeenten om zo een centraal beeld op te bouwen van de stand van zaken van de kwetsbaarheid en de eventuele oplossing. Daar waar gemeenten zelf geen contact kregen met leveranciers is ook namens gemeenten aangedrongen op een oplossing. De focus op leveranciers leverde ook nieuwe relaties op tussen de IBD en leveranciers waartussen eerder geen contact was. Het is overigens niet bij alle aangeschreven leveranciers gelukt om contact te krijgen. Het gezamenlijke beeld is dagelijks gedeeld met de vertrouwde contactpersonen van gemeenten.
Om gemeenten in staat te stellen om kennis en informatie uit te wisselen organiseerde de IBD een samenwerkingsruimte en een dagelijks spreekuur. Ten slotte bood de IBD technisch advies, hulp en ondersteuning bij detectie en monitoring en scande de IBD gemeenten die daar toestemming voor gaven actief op aanwezigheid van de kwetsbaarheid. De werkzaamheden leidden ertoe dat de IBD-CERT tijdelijk is opgeschaald met andere adviseurs uit het team van de IBD. Om de tevredenheid van gemeenten te meten voerde de IBD een enquête uit. Gemeenten gaven aan in het algemeen tevreden te zijn met de informatievoorziening en de verbindende rol van de IBD. Het commentaar van gemeenten is verwerkt in onderstaande dilemma's.

Dilemma's

Gewicht adviezen van de IBD

In situaties als met Log4shell adviseert de IBD gemeenten over preventie, detectie, oplossing en herstel. De IBD publiceerde bij Log4shell een afwegingskader waarmee keuzes over maatregelen inzichtelijk werden. Bij een aanwezige kwetsbaarheid was het de keuze tussen bijwerken, afschermen of uitschakelen. Het komt regelmatig voor dat gemeenten om 'hardere' adviezen vragen waarbij de IBD adviseert om systeem x van leverancier y uit te zetten. Elke gemeente is echter anders. Voor de ene gemeente zijn de adviezen onverkort van toepassing, voor de andere zijn de adviezen te zwaar of te licht. Het is altijd van belang dat gemeenten zoveel mogelijk zelf afwegingen maken. Het kan echter voorkomen dat acute dwingende adviezen nodig zijn. Om te voorkomen dat de IBD afwegingen op lokaal niveau laat waar deze eigenlijk collectief gemaakt zouden moeten worden, is het van belang dat er een snelle toetsingsmogelijkheid komt waarbij directie en bestuur van gemeenten zeggenschap hebben over de zwaarte van adviezen.

Informatievoorziening richting directie van gemeenten

De IBD krijgt naast informatie voor de doelgroep van informatiebeveiligingsfunctionarissen ook informatie van strategische en tactische aard. Zo deelde de rijksoverheid een set aan scenario's voor het verloop van de ontwikkelingen rond Log4shell. In het worst-case scenario zou sprake zijn van maatschappelijke ontwrichting. De IBD heeft hierop deze informatie via de vakvereniging van gemeentesecretarissen gedeeld met de directie van gemeenten. De reacties hierop waren overwegend positief, echter gaven enkele grote gemeenten aan dat ze hier eerder last dan gemak van hadden. De IBD zal samen met gemeenten kijken of en hoe de informatievoorziening naar de directie op een optimale manier kan worden ingericht.

Detectie en toestemming daarvoor

De IBD werkt in 2022 aan een pilot om de informatievoorziening van gemeenten actief te scannen op de aanwezigheid van kwetsbaarheden en risicovolle configuraties. In december 2021 was deze pilot in voorbereiding en deed zich de kans voor om te scannen op de Log4j-kwetsbaarheid. De IBD heeft hiervoor toestemming gevraagd aan gemeenten, die op hun beurt weer toestemming dienden te verlenen namens hun leveranciers. De scan van de IBD was van eenzelfde aard als de scans van criminelen, onderzoekers en statelijke actoren – met dien verstande dat de IBD met de resultaten gemeenten waarschuwt. Ook hier waren de reacties overwegend positief of neutraal. In enkele gevallen gaven gemeenten aan dat de vraag om toestemming niet wenselijk was. De IBD kijkt samen met gemeenten of en hoe het mandaat om te scannen kan worden ingericht.

Vertrouwelijkheid bij samenwerking tussen honderden contacten

Bij de Log4j- kwetsbaarheden verzamelde de IBD informatie van vertrouwelijke aard. Met name informatie over kwetsbaarheden bij leveranciers zijn om redenen van veiligheid en commerciële redenen niet openbaar. Bij de inrichting van de samenwerkingsruimte en dagelijkse spreekuren waren honderden contacten betrokken. De hoeveelheid contacten vergrootte de kans dat informatie (bedoeld of onbedoeld) op plekken terecht kwam waar dat niet de bedoeling was. De IBD zoekt samen met de doelgroep naar manieren om risico's rond vertrouwelijkheid in toekomstige situaties te beheersen.

Collectief leveranciersmanagement

De VNG/IBD heeft geen formele rol in de relatie tussen leveranciers en gemeenten. Op basis van de goede relatie kon de IBD informatie ophalen en namens gemeenten sturen op een oplossing bij leveranciers. Gemeenten en leveranciers hebben baat bij een gezamenlijke aanpak en een eenduidig beeld bij een oplossing. De collectieve aanpak van gemeenten dient natuurlijk breder te zijn dan alleen het thema informatiebeveiliging. De IBD voert hierover het gesprek met de VNG collega's van markt en overheid. Dit team M&O zet zich in de breedte in om gemeenten te helpen om goed opdrachtgeverschap vorm te geven.

Aanbevelingen gemeenten

In aanvulling op de aanbeveling om de basis op orde[11] te hebben en te houden identificeerden de IBD en gemeenten de navolgende aanvullende aanbevelingen als gevolg van Log4shell:

Houd de crisisorganisatie paraat, organiseer de bereikbaarheid voor spoedgevallen

Als gemeenten het hebben over de crisisorganisatie dan is dit vaak in de context van incidenten: een hack, een datalek of een storing. Bij Log4shell bleek de crisisstructuur ook zinvol bij de aansturing en coördinatie van preventieve acties (het oplossen van kwetsbaarheden). De IBD raadt gemeenten aan om de eigen aanpak te evalueren en verbeterpunten te verwerken in het eigen crisis- en /of incidentmanagementplan.

Samenwerking en vertrouwen

Het blijkt dat in de samenwerking met leveranciers weinig gedetailleerde afspraken zijn over informatiebeveiliging en privacy. Ook is er weinig toezicht op de naleving van de afspraken die er wel zijn. Er is sprake van veel vertrouwen dat partijen allemaal een belang hebben bij een veilige digitale omgeving. Tijdens een dergelijke kwestie ontstaat opeens een verhoogde interesse in de stand van zaken en dan pas blijkt of het eerdere vertrouwen terecht is. De IBD adviseert gemeenten om regelmatig (en dus buiten crisistijd) het gesprek te voeren over de risico's rond digitale veiligheid en privacy. Hierbij kunnen bestaande afspraken tegen het licht gehouden worden en waar nodig kunnen deze worden geactualiseerd. Als blijkt dat extra controle in de vorm van bijvoorbeeld een penetratietest nodig is, verdient het aanbeveling om deze collectief te organiseren.

Actualiseer de ICT-foto en de IP-gegevens bij de IBD

De IBD kan gemeenten (kwetsbaarheids)waarschuwingen op maat sturen als de gemeente aangeeft over welke hard- en software men wil worden geïnformeerd. Ook kan de IBD gericht gemeenten waarschuwen als de IP-adressen en domeinnamen van de gemeente bekend zijn. Bij Log4shell had de IBD via partners veel informatie over IP-adressen van kwetsbare systemen, die we filterden op gemeentelijke adressen. Hoe nauwkeuriger en actueler de gemeente degegevens aanlevert, hoe beter de IBD haar rol kan invullen.

Laat gemeenschappelijke regelingen aansluiten bij de IBD

De IBD onderhoudt primair het contact met gemeenten. Voor gevallen waarin gemeentelijke taken in een samenwerkingsverband worden uitgevoerd is het ook mogelijk voor gemeenschappelijke regelingen om gebruik te maken van de dienstverlening van de IBD. De IBD raadt gemeenten aan om de eigen gemeenschappelijke regelingen te laten aansluiten. Dat kan eenvoudig door contactpersonen aan te stellen en de ICT-foto en IP-adresgegevens aan te leveren. Zo zijn gemeenten er zeker van dat belangrijke informatie over informatiebeveiliging en privacy ook tijdig bij de samenwerkingen bekend is.

Links in dit document

1 https://www.ncsc.nl/actueel/nieuws/2021/december/10/ernstige-kwetsbaarheid-in-apache-Log4j
2 De component komt voor in hard- en software. Bij hardware gaat het om de softwarebesturing. Vandaar dat we in de rest van dit document vooral de term software gebruiken.
3 https://www.informatiebeveiligingsdienst.nl/nieuws/jaaroverzicht-2021/
4 https://nl.wikipedia.org/wiki/Heartbleed
5 Het woord leveranciers kan breed uitgelegd worden, het kan hierbij gaan om aanbieders van software, aanbieders van clouddiensten maar ook om onderaannemers / ketenpartners en landelijke overheidsvoorzieningen. Voor de leesbaarheid noemen we deze leveranciers.
6 Zie de paragraaf **Collectieve aanpak**
7 https://www.ncsc.nl/actueel/nieuws/2022/januari/20/houd-aandacht-voor-Log4j
8 Zie de paragraaf **Aanbevelingen voor gemeenten**
9 https://www.informatiebeveiligingsdienst.nl/nieuws/kwetsbare-log4j-applicaties-en-te-nemen-stappen/
10 Zie de paragraaf **Dilemma's**
11 In het geval van Log4shell zijn de basisprocessen configuratiemanagement en patchmanagement essentieel. Het ondersteuningsprogramma Verhogen Digitale Weerbaarheid (VDW) helpt hierbij: https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/

Meer informatie

Meer informatie over onze dienstverlening vindt u in de andere factsheets van de IBD en op de website www.informatiebeveiligingsdienst.nl. De helpdesk van de IBD is te bereiken tijdens kantooruren van 9:00 tot 17:00 uur op het nummer 070 204 55 11 of via het e-mailadres info@IBDgemeenten.nl. De CERT van de IBD is 24x7 bereikbaar via 070 204 55 11 (instructies voor het piketnummer op de voicemail).