Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 814

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID, DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 december 2021

Met deze brief informeren wij uw Kamer over de geconstateerde kwetsbaarheid in Apache Log4j, en de waarschuwing en het advies dat het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Justitie en Veiligheid daarover heeft gegeven aan rijksoverheid en vitale aanbieders.

Daarnaast informeren wij uw Kamer over de tot op heden genomen maatregelen en voorziene vervolgstappen. Het kabinet neemt deze kwetsbaarheid zeer serieus.

Aanleiding

Er is een ernstige kwetsbaarheid gevonden in Apache Log4j. Dit is een veelvuldig gebruikte softwaremodule in ICT-systemen en daarmee zeer breed in gebruik bij grote en kleine organisaties in binnen- en buitenland, binnen en buiten de doelgroep van het NCSC (rijksoverheid en vitale aanbieders).

Omdat veel organisaties in Nederland en daarbuiten gebruik maken van Apache Log4j kan de impact van misbruik van deze kwetsbaarheid groot zijn. Het is een softwaremodule die gebruikt wordt in diverse applicaties, waaronder webapplicaties. Specifiek wordt deze software gebruikt voor het bijhouden van digitale logboeken. Het treffen van mitigerende maatregelen voor organisaties is complex en tijdrovend. Het is lastig vast te stellen welke systemen en organisaties kwetsbaar zijn en wat de potentiële operationele impact is als de kwetsbaarheid zou worden misbruikt.

kst-26643-814
ISSN 0921 - 7371
's-Gravenhage 2021

Rollen en verantwoordelijkheden

Binnen de rijksoverheid zijn meerdere organisaties bij de aanpak van de Apache Log4j kwetsbaarheid betrokken die nauw samenwerken vanuit hun eigen rollen en taken. De Minister van Justitie en Veiligheid is coördinerend bewindspersoon voor cybersecurity. Onderdeel van zijn ministerie is het NCSC, dat primair tot taak heeft om vitale aanbieders en rijksoverheidsorganisaties te informeren en adviseren over dreigingen en incidenten betreffende hun systemen. De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties is stelselverantwoordelijk voor de digitale veiligheid van het openbaar bestuur en coördinerend verantwoordelijk voor informatiebeveiliging bij het Rijk.
Vanuit die verantwoordelijkheden wordt er bij de departementen en koepelorganisaties van de medeoverheden gemonitord op de genomen maatregelen. De Minister van Economische Zaken (EZK)coördineert het beleid op de digitale economie en overkoepelende digitaliseringsstrategie, en is verantwoordelijk voor het Digital Trust Center (DTC) die het niet-vitale bedrijfsleven informeert en adviseert om hun digitale weerbaarheid te verhogen.

Genomen stappen

De afgelopen dagen is onder coördinatie van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) door het NCSC en BZK intensief samengewerkt met alle betrokken vakdepartementen, medeoverheden, diverse (vitale en niet-vitale) aanbieders en andere organisaties binnen de cybersecuritygemeenschap.

Op 10 december jl. heeft het NCSC het eerste algemene beveiligingsadvies voor deze kwetsbaarheid op haar website gepubliceerd. Het NCSC waarschuwt daarin voor potentieel grote schade en adviseert organisaties daarom zich voor te bereiden op een mogelijke aanval. Daarbij is aangegeven dat het zeer waarschijnlijk is dat in de komende weken digitale (ransomware)aanvallen en datalekken plaatsvinden.

Het NCSC heeft actief rijksoverheidsorganisaties, vitale aanbieders en andere schakelorganisaties binnen het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden geïnformeerd middels een beveiligingsadvies en een doelgroepenbericht. Ook de toezichthouders zijn geïnformeerd. Het NCSC, DTC en CSIRT-DSP hebben daarnaast op 15 december jl. een gezamenlijk Webinar voor IT-specialisten gehost over Log4j met ongeveer 2400 deelnemers die honderden vragen hebben gesteld die zo veel als mogelijk zijn beantwoord.

Door het NCSC is voorts een stappenplan ontwikkeld en een publiek platform gestart, waarop een lijst openbaar is gemaakt van kwetsbare applicaties. Nationale en internationale partners en andere organisaties zijn gevraagd om aanvullende informatie hierover te delen. Dat wordt massaal gedaan. Daarnaast zijn er vanaf 10 december jl. door het NCSC en DTC diverse calls en webinars georganiseerd met Computer Emergency Response Teams en andere (doelgroep)organisaties om hen zo veel als mogelijk te informeren over de kwetsbaarheid Log4j, over daarvoor mogelijk te nemen maatregelen en om input op te halen voor een landelijk beeld.

Vanuit het Ministerie van BZK heeft de Chief Information Security Officer Rijk (CISO Rijk) nauw contact met alle departementen om te zorgen dat de maatregelen en het stappenplan van het NCSC worden opgevolgd en er doorlopend onderzoek plaatsvindt op mogelijk misbruik.

Hetzelfde geldt voor de medeoverheden. Provincies, gemeenten en waterschappen voeren maatregelen uit en de sectorale Computer Emergency Response Team's (CERT's) zijn alert en informeren de bij hun aangesloten medeoverheden proactief.

Vervolg

Vanaf het bekend worden van de kwetsbaarheid heeft het NCSC de situatie doorlopend gemonitord, adviezen geactualiseerd en nauw contact onderhouden met Rijksorganisaties, vitale aanbieders en cybersecurity-partners in binnen- en buitenland. Op de website van het NCSC wordt steeds het meest actuele algemene handelingsperspectief gepubliceerd. Ook het DTC communiceert de meest actuele informatie en handelingsperspectieven naar haar doelgroep.

Vanzelfsprekend is er ook aandacht voor de mogelijkheid dat de vitale infrastructuur of dat vitale belangen geraakt worden. Verstoring van een vitaal proces kan de continuïteit van dit proces ernstig raken.

De komende dagen zal het beeld ten aanzien van de impact van de gevonden kwetsbaarheid in Log4j nader worden geduid. Ook zal door onze ministeries worden gewerkt aan een handelingsperspectief in het kader van de uitoefening van de respectievelijke taken van de ministeries, indien en voor zover de kwestie zich langer zal voordoen.
Deze kwetsbaarheid toont weer aan hoe belangrijk onze digitale veiligheid is. Het kabinet werkt daarom aan de versterking van de digitale weerbaarheid via de Nederlandse Cyber Security Agenda (NCSA). Desondanks neemt het dreigingsniveau toe, zoals ook blijkt uit het Cybersecurity Beeld Nederland van 28 juni 2021 (Kamerstuk 26 643, nr. 767). Dat is zorgwekkend, zeker in combinatie met onze afhankelijkheid van digitale systemen. Het is daarom van groot belang dat ook het volgende kabinet inzet op het versterken van de digitale weerbaarheid van Nederland.

Waar nodig blijven wij de komende periode uw Kamer informeren.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops

De Minister van Economische Zaken en Klimaat,
S.A. Blok