Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 658

BRIEF VAN DE MINISTERS VAN JUSTITIE EN VEILIGHEID EN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 januari 2020

Met deze brief informeren wij uw Kamer over de geconstateerde kwetsbaarheid in Citrix producten en de waarschuwing en het advies dat het Nationaal Cyber Security Centrum (NCSC) daarover heeft gegeven aan rijksoverheid en vitale aanbieders. Daarnaast informeren wij uw Kamer over de tot op heden genomen maatregelen en vervolgstappen die nu gezet worden.

Het Kabinet neemt deze kwetsbaarheid zeer serieus. De afgelopen dagen is onder onze coördinatie, via de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), het Nationaal Cyber Security Centrum en CIO-Rijk intensief samengewerkt met alle betrokken vakdepartementen en organisaties. De situatie wordt doorlopend gemonitord. Veel organisaties in Nederland en daarbuiten maken gebruik van Citrix producten en hierdoor kan de impact van misbruik van deze kwetsbaarheid groot zijn. Specifiek gaat het om de kwetsbaarheid in de volgende Citrix producten: ADC, Citrix Gatewayservers, voorheen bekend als Citrix Netscaler. Deze programma's worden onder andere gebruikt om externe toegang tot een netwerk mogelijk te maken, bijvoorbeeld voor thuiswerken en in sommige gevallen primaire processen. De potentiële impact van de kwetsbaarheid en impact is in dit laatstgenoemde, specifieke geval groot, omdat (1) veel organisaties maken gebruik van deze systemen, (2) de kwetsbaarheid breed bekend is en (3) Citrix nog geen sluitende oplossing kan bieden.

Op 17 december 2019 maakte Citrix bekend dat er sprake was van een kwetsbaarheid in de genoemde Citrix producten. Het NCSC heeft daarom op 18 december 2019 een eerste beveiligingsadvies voor deze kwetsbaarheid gepubliceerd. Op 24 december 2019 heeft het NCSC de inschaling verhoogd naar het allerhoogste niveau (high/high) op basis van nieuwe informatie en technische analyses. Duidelijk was bovendien dat de beschikbaarheid van beveiligingsupdates vanuit Citrix niet op korte termijn voor handen zouden zijn. De waarschuwingen gelden voor de doelgroepen van het NCSC (Rijk en Vitaal) en wordt ten behoeve van het

kst-26643-658
ISSN 0921 - 7371
's-Gravenhage 2020

overige bedrijfsleven en overige organisaties gedeeld met onder meer het Digital Trust Center (DTC) voor het bedrijven in Nederland en andere CERT's (Computer Emergency Response Teams) zoals bijvoorbeeld Z-CERT voor zorginstellingen en de Informatiebeveiligingsdienst voor gemeenten (IBD). Vanaf het bekend worden van de kwetsbaarheid heeft het NCSC de situatie doorlopend gemonitord, adviezen geactualiseerd en nauw contact onderhouden met Rijksorganisaties en vitale aanbieders. Over de in die periode genomen maatregelen zou uw Kamer nader geïnformeerd kunnen worden door middel van een technische briefing.

In de periode van 9 tot 17 januari 2020 werd bekend dat er een zogenaamde exploitcode (waarmee de kwetsbaarheid kan worden misbruikt) publiekelijk beschikbaar was en werd duidelijk dat aanvallers actief zochten naar kwetsbare systemen. In de week van 13 tot en met 17 januari 2020 is daarnaast uit intensieve contacten met Citrix duidelijk geworden dat Citrix op korte termijn geen sluitende oplossing kon bieden.

Op vrijdag 17 januari 2020 bracht de AIVD een beveiligingsadvies uit. Op basis van de ontstane situatie en het beveiligingsadvies is daarom op 17 januari jl. – door het NCSC – het dringende advies gegeven aan rijksoverheid en het advies aan vitale organisaties om de Citrix-systemen uit te schakelen tot het moment dat een sluitende oplossing beschikbaar is. Voorafgaand aan de publicatie van het advies, is vrijdagavond contact met u opgenomen om de Kamer hierover te informeren. Aan organisaties binnen de rijksoverheid is door het NCSC of CIO-Rijk geadviseerd systemen uit te schakelen, tenzij aan de volgende, cumulatieve voorwaarden wordt voldaan:

1. uitschakeling disproportionele gevolgen heeft, bijvoorbeeld voor de veiligheid en gezondheid; en
2. Als er afdoende extra monitorings- en beveiligingsmaatregelen kunnen worden genomen; en
3. Systemen effectief kunnen worden gecompartimenteerd of in quarantaine gezet kunnen worden, er voldoende detectie mogelijk zijn en contaminatie van de eigen systemen en die van anderen uitgesloten kan worden.

Het is aan organisaties zelf om af te wegen wat de impact is op basis van deze genoemde criteria. Indien organisaties besluiten om Citrix-systemen niet uit te schakelen, adviseert het NCSC met klem de genoemde aanvullende maatregelen te nemen, bovenop de door Citrix geadviseerde maatregelen gepubliceerd op de website van Citrix. Op basis van dit advies hebben veel organisaties zelf de afweging gemaakt en in sommige gevallen besloten om Citrix-systemen uit te schakelen. Het beeld bij de overheid (Rijk, provincies, gemeenten en waterschappen) is dat het advies van het NCSC grotendeels is overgenomen en dat organisaties op basis van een risico-afweging in sommige gevallen hebben besloten Citrix (deels) op een gecontroleerde manier te laten draaien.

Voor de rijksoverheid beoordeelt de Chief Information Officer (CIO) Rijk in overleg met de organisaties binnen de rijksoverheid welke systemen er worden uitgeschakeld dan wel welke systemen blijven draaien, alsook of de ad. 2 en 3 bedoelde maatregelen ten aanzien van die systemen adequaat genomen zijn. Voor de vitale aanbieders geldt dat het NCSC in nauw contact blijft en hulp aanbiedt waar mogelijk. Voor organisaties die buiten de doelgroep van het NCSC vallen, informeert het NCSC informatieknooppunten, zoals het DTC en andere CERTS.

Het NCSC blijft de situatie nauwlettend monitoren en blijft in contact met Citrix, haar doelgroepen en (internationale) partners. Het NCSC zal net als afgelopen dagen de adviezen steeds blijven actualiseren.

Op de avond van 19 januari jl. heeft Citrix de eerste patches beschikbaar gemaakt. Organisaties worden met klem geadviseerd de patches uit te voeren, maar wel de afweging te maken wat de impact is en of (aanvullende) maatregelen alsnog nodig blijven cq. zijn. Het NCSC adviseert daarbij over het doorvoeren van de patches. Voor andere versies van Citrix-systemen worden op korte termijn patches verwacht. Zodra Citrix patches beschikbaar stelt, adviseren de Rijks-CIO en NCSC in hoeverre de maatregelen kunnen worden afgeschaald.

Dit soort kwetsbaarheden tonen hoe belangrijk onze digitale veiligheid is. Het kabinet werkt aan de versterking van onze digitale weerbaarheid, vandaar ook dat dit kabinet voor het eerst een Nederlandse CyberSecurity Agenda heeft opgesteld.[1] Op korte termijn zal het kabinet uw Kamer informeren over wat deze specifieke kwetsbaarheid ons daarbij leert, ook in relatie tot de in voorbereiding zijnde kabinetsreactie op het WRR-rapport «Voorbereiden op Digitale Ontwrichting».

Over de huidige Citrix kwetsbaarheid bieden wij uw Kamer graag op korte termijn aan een technische briefing te verzorgen. De komende dagen blijven wij uw Kamer informeren.

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

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

[1] Kamerstuk 26 643, nr. 614 en Kamerstuk 26 643, nr. 647.