Ministerie van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Ons kenmerk
2806738

Datum 23 januari 2020
Onderwerp Overzicht op hoofdlijnen Citrix-kwetsbaarheden

Met deze brief informeren wij uw Kamer, naar aanleiding van het Mondeling Vragenuur van 21 januari jongstleden over belangrijkste feiten en ontwikkelingen voorafgaand aan de technische briefing over Citrix-kwetsbaarheden die u op ons aanbod op donderdag 23 januari ontvangt. Dit in aanvulling op de brief hierover die uw Kamer 20 januari jl. ontving.[1]

Rolverdeling betrokken organisaties
Binnen de Rijksoverheid zijn meerdere organisaties bij de Citrix-kwetsbaarheid betrokken die nauw samenwerken vanuit hun eigen rollen en taken. Departementen hebben een eigen verantwoordelijkheid voor hun ICT-systemen. De ministeries van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties hebben daarnaast een systeemverantwoordelijkheid. Hieronder een beschrijving van hun rol bij de Citrix-kwetsbaarheid en vergelijkbare situaties.

Om dit overzicht van de belangrijkste feiten zo begrijpelijk mogelijk te maken, schetsen wij eerst in het kort de rolververdeling van de belangrijkste betrokken organisaties.

JenV
Het ministerie van Justitie en Veiligheid is coördinerend ministerie op het gebied van cybersecurity in generieke zin. Het NCSC en de NCTV maken onderdeel uit van dit ministerie.

NCSC
Met het oog op het voorkomen en beperken van maatschappelijke ontwrichting door cyberdreigingen en –incidenten en het versterken van de digitale weerbaarheid in de samenleving, heeft het NCSC tot wettelijke taak de Rijksoverheid en vitale aanbieders te informeren en te adviseren over dreigingen en incidenten met betrekking tot hun informatiesystemen. Het NCSC staat Rijksoverheids en vitale aanbieders bij in het treffen van maatregelen om de continuïteit van hun diensten te waarborgen. Daarnaast verricht het NCSC

[1] Kamerstuk 26643-658.

analyses en technisch onderzoek, om de Rijksoverheid en vitale organisaties te kunnen informeren en adviseren.

Het NCSC heeft een operationeel coördinerende rol binnen de nationale crisisstructuur. Het NCSC kan niet afdwingen dat een rijksoverheidsorganisatie of vitale aanbieder zich laat bijstaan of zich laat informeren of adviseren. Opvolging van adviezen van het NCSC is de verantwoordelijkheid van organisaties zelf.

NCTV
De NCTV is de nationale crisis coördinator en vanuit die rol betrokken bij incidenten, calamiteiten en crises. Het NCTV coördineert de interdepartementale afstemming en opschaling en waar nodig in samenwerking met andere organisaties.

BZK
Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor het rijksbrede informatiebeveiligingsbeleid.

CIO-Rijk
De CIO-Rijk heeft binnen het Rijk een belangrijke rol op het gebied van informatiebeveiliging. De CIO-Rijk stelt kaders en richtlijnen voor het niveau van digitale beveiliging middels de Baseline Informatiebeveiliging Overheid (BIO). Daarnaast kan de CIO-Rijk in gevallen als de Citrix-kwetsbaarheid vragen om beveiligingsadviezen op te volgen middels het 'comply or explain' principe.

Informatie van Citrix
Op 17 december 2019 maakte Citrix publiekelijk bekend dat er een kwetsbaarheid in Citrix ADC en Citrix Gateway (voorheen bekend als Netscaler) geconstateerd was.[2] Dit was het eerste tijdstip waarop het Nationaal Cyber Security Centrum (NCSC) hiervan op de hoogte werd gesteld.[3]

Bij het publiekelijk bekend maken van de kwetsbaarheid op 17 december 2019 adviseerde Citrix zelf aan alle gebruikers van de betreffende systemen een aantal tussentijdse mitigerende maatregelen te nemen. Er was op het moment van bekendmaking van de kwetsbaarheid dus geen definitieve oplossing beschikbaar.

Op 11 januari 2020 heeft Citrix publiekelijk een tijdlijn gecommuniceerd m.b.t. het beschikbaar komen van de onderscheiden patches voor de verschillende versie van de Citrix-producten. Deze tijdlijn is later bijgesteld. Op maandag 20 januari 2020 zijn de eerste patches beschikbaar gemaakt door Citrix. Deze bieden een oplossing voor ongeveer 50 procent van de kwetsbare Citrix-systemen in Nederland. Na contact tussen NCSC en Citrix zijn de patchmomenten naar voren gehaald. Citrix verwacht de overige benodigde patches op vrijdag 24 januari, 23.00 uur Nederlandse tijd, beschikbaar te maken.

Adviezen en maatregelen van het Nationaal Cyber Security Centrum (NCSC) en CIO-Rijk
Kwetsbaarheden worden door het NCSC behandeld aan de hand van een gestandaardiseerd model. Het NCSC heeft de Citrix-kwetsbaarheid aanvankelijk ingeschaald op middel/hoog risico, en later dit bijgesteld naar de hoogste classificatie. Vanaf de bekendmaking van de kwetsbaarheid door Citrix op 17 december heeft het NCSC continu gemonitord, technisch onderzoek verricht, (beveiligings)adviezen uitgebracht en waar nodig bijstand verleend aan de Rijksoverheid en vitale aanbieders. Daartoe behoorde ook het adviseren van

[2] Verder in deze brief aangeduid met: Citrix-systemen.
[3] Citrix maakte op 18 januari in een uitzending van Nieuwsuur bekend dat Citrix op 6 december door beveiligingsonderzoekers over de kwetsbaarheid op de hoogte is gesteld. Dit heeft Citrix nadien desgevraagd bij het NCSC bevestigd.

aanvullende maatregelen van het NCSC. De doelgroepen van het NCSC, de Rijksoverheid en vitale aanbieders, zijn doorlopend benaderd door het NCSC bij adviezen en updates. Daarnaast heeft het NCSC informatieknooppunten en computercrisisteams op meerdere momenten geïnformeerd, zodat die de beveiligingsadviezen verder kunnen verspreiden onder organisaties buiten de doelgroep van het NCSC. De beveiligingsadviezen van het NCSC worden altijd op de website van het NCSC gepubliceerd voor een breder publiek.

Hieronder volgt een opsomming van de belangrijkste momenten:
Na de bekendmaking van de kwetsbaarheid door Citrix, heeft het NCSC op 18 december 2019 een eerste beveiligingsadvies t.a.v. deze kwetsbaarheid uitgebracht (medium/high).

Op 24 december 2019 heeft het NCSC de inschaling van deze kwetsbaarheid verhoogd naar het allerhoogste niveau (high/high: hoge kans op misbruik én hoge impact bij misbruik) op basis van nieuwe informatie en technische analyses. Het NCSC heeft vervolgens dezelfde dag en de dagen erna contact gezocht met de doelgroeporganisaties die bij het NCSC hadden aangegeven deze software te gebruiken om hen te alerteren op dit beveiligingsadvies.

Op 9 januari 2020 bleek dat er op korte termijn zeer waarschijnlijk een zogeheten *exploitcode* publiekelijk bekend zou worden, waarmee de kwetsbaarheid kan worden misbruikt. Tevens werd bekend dat er actief werd gezocht naar kwetsbare systemen, potentieel door kwaadwillenden. Op 11 januari constateerde het NCSC dat de exploitcode ook daadwerkelijk gepubliceerd was. Het NCSC heeft zowel op 9 als 11 januari zijn advies geactualiseerd en organisaties binnen Rijk en vitaal actief geïnformeerd over deze nieuwe ontwikkelingen en geadviseerd om zo snel mogelijk de door Citrix geadviseerde mitigerende maatregelen te nemen.

Op 10 januari 2020 heeft CIO Rijk op verzoek van het NCSC de CTO's en CISO's[4] van alle departementen van de Rijksoverheid aanvullend geïnformeerd over de Citrix-kwetsbaarheid, en daarbij verzocht hierover terug te melden. CIO Rijk heeft er daarbij op aangedrongen of de departementen de door Citrix geadviseerde tussentijdse mitigerende maatregelen hadden getroffen en in de dagen hierna is hierover contact geweest met die organisaties.

Op 13 januari 2020 constateerde het NCSC dat er nog altijd veel Citrix-systemen in Nederland kwetsbaar waren. Het NCSC heeft daarom een bericht op haar website en social media geplaatst om hier voor te waarschuwen. Doelgroeporganisaties van het NCSC zijn opnieuw actief geïnformeerd. Bovendien zijn de sectorale toezichthouders op de hoogte gesteld.

Op 16 januari 2020 was er ten eerste nog altijd geen zekerheid dat er op zeer korte termijn een sluitende oplossing door Citrix beschikbaar gesteld zou worden. Ten tweede beoordeelde het NCSC mede op basis van informatie van specialisten dat de effectiviteit van de tussentijdse mitigerende maatregelen van Citrix onvoldoende zekerheid kon bieden. Ten derde bleken er nog steeds organisaties die de tussentijdse mitigerende maatregelen van Citrix niet of in onvoldoende mate hadden genomen. Het NCSC heeft diezelfde dag bij haar doelgroepen aangegeven dat het onduidelijk is of de tussentijdse mitigerende maatregelen van Citrix in alle gevallen effectief zijn voor het voorkomen van misbruik. Naast de eerder aangegeven aanvullende beveiligingsmaatregelen heeft het NCSC geadviseerd te overwegen om systemen met de betreffende Citrixproducten uit te schakelen en waar mogelijk de aanvullende maatregelen te treffen. Het nieuwe advies van het NCSC was aanleiding voor de NCTV om interdepartementaal op te schalen.

[4] Chief Information Officer (CIO), Chief Technology Officer (CTO) en Chief Information Security Officer (CISO).

Op 17 januari 2020 heeft de NCTV een overleg belegd met alle departementen over de ontstane situatie. Diezelfde dag bracht de AIVD een beveiligingsadvies uit. Op basis van de op dat moment beschikbare informatie is door ons akkoord gegeven aan het NCSC om het dringende advies uit te brengen aan Rijksoverheid en het advies aan vitale organisaties om de Citrix-systemen uit te schakelen tot het moment dat een sluitende oplossing beschikbaar is, waarbij het NCSC tevens heeft geadviseerd om het belang van de continuïteit van primaire processen af te wegen tegen eventuele negatieve gevolgen. Dit advies van het NCSC is bovendien breder verspreid via een persbericht op rijksoverheid.nl, de website van het NCSC en via andere cybersecurity-organisaties in Nederland.

Naar aanleiding van de opschaling op 17 januari 2020 door NCTV en het overleg tussen de bewindspersonen, heeft CIO Rijk de departementen gevraagd om Citrix-systemen uit te schakelen, tenzij aan drie cumulatieve voorwaarden wordt voldaan (zie onder *Beveiligingsmaatregelen*).

Op basis hiervan hebben de overheidsorganisaties bij het Rijk (departementen en uitvoeringsorganisaties) vervolgens zelf een risicoafweging gemaakt over het al dan niet uitschakelen van de betreffende Citrix-producten. CIO Rijk heeft doorlopend contact gehad met de departementen over de opvolging van het beveiligingsadvies. Hierbij is het principe gehanteerd 'comply or explain' aan de CIO Rijk. CIO Rijk heeft de departementen gevraagd om de uitkomsten van die risicoafweging (Citrix-systemen aan of uit) terug te koppelen. CIO Rijk monitort hoe hier binnen de Rijksoverheid en op hoofdlijnen bij de medeoverheden opvolging wordt gegeven aan het advies.

Op 19 januari zijn vanuit Citrix de eerste patches beschikbaar gesteld voor een deel van de kwetsbare softwarepakketten. Het NCSC heeft haar beveiligingsadvies dezelfde dag hierop aangevuld en doelgroepen hierop gewezen. Daarnaast is het brede publiek hier over geïnformeerd via de website. Het NCSC coördineert de controle op de effectiviteit van de patches.

Op 21 januari heeft het NCSC op zijn website voor het brede publiek een Frequently Asked Questions geplaatst ten aanzien van de Citrix-kwetsbaarheid.

Het NCSC heeft doorlopend contact met Citrix over de ontwikkelingen. Het NCSC blijft de ontwikkelingen rond de kwetsbaarheid en het beschikbaar komen van de patches nauwgezet monitoren en zal haar berichtgeving hierop bijwerken. Daarnaast staat het NCSC, waar nodig, zijn doelgroep bij op dit moment. Zoals toegezegd tijdens het mondelinge vragenuur op 21 januari volgt bij de kabinetsreactie op het WRR-rapport 'Voorbereiden op Digitale Ontwrichting' een evaluatie waarin de adviezen, maatregelen en de opvolging daarvan vanaf het bekend worden van de kwetsbaarheid zullen worden betrokken.

Informatievoorziening en communicatie breder publiek
Het NCSC publiceert zijn beveiligingsadviezen standaard op de NCSC-website. Met betrekking tot de Citrix-kwetsbaarheid heeft het NCSC daarnaast actief nieuwsberichten op de website geplaatst en social media-berichten gepubliceerd. Daarbij heeft het NCSC ook doorlopend samenwerkingspartners, zoals het DTC, geïnformeerd over de ontwikkelingen, zodat zij hun eigen doelgroep actief konden benaderen. Specifiek op vrijdag 17 december is een persbericht geplaatst op de website van de Rijksoverheid.

Beveiligingsmaatregelen
Zoals hierboven beschreven heeft Citrix als tijdelijke oplossing voor de kwetsbaarheid steeds tussentijdse mitigerende maatregelen aanbevolen. Toen het NCSC beoordeelde dat de effectiviteit van de tussentijdse maatregelen onvoldoende zekerheid bood, heeft het NCSC aanvullende beveiligingsmaatregelen aanbevolen, waaronder IP-whitelisting en het instellen van een zogeheten webapplicatiefirewall.

Verder zijn organisaties op 17 januari geadviseerd om de Citrix-systemen af te schakelen, tenzij aan drie cumulatieve voorwaarden kan worden voldaan:

1. Uitschakeling heeft disproportionele gevolgen, bijvoorbeeld voor de veiligheid en gezondheid; en

2. Er afdoende extra monitorings- en beveiligingsmaatregelen kunnen worden genomen; en

3. Systemen effectief 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.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

Raymond Knops