# Even snel de Citrix ADC-server patchen is niet de hele oplossing

**De afgelopen week heeft het probleem met de onveilige Citrix ADC servers Nederland bezig gehouden. Op deze website waarschuwde ik er op 14 januari 2020 ook voor. Opeen was thuis werken met inloggen op de systemen van de baas niet meer mogelijk in veel gevallen. Zelfs het woord "Citrix-file" ontstond. Het is de benaming voor de autofiles die vandaag langer zijn door werknemers die naar kantoor gaan i.p.v. op afstand inloggen. Vanaf vandaag levert Citrix software patches uit om de kwetsbaarheid CVE-2019-19781 te repareren.** Die patches zijn niet voor alle kwetsbare apparaten. Voor een deel moeten de patches deze week nog komen. Citrix zegt de uiterste termijn van 31 januari naar 24 januari naar voren gehaald te hebben. Het bedrijf waarschuwt ervoor zeer zorgvuldig op te letten dat men de juiste patch voor het juiste apparaat gebruikt. Daarnaast heeft ook het Nationaal Cyber Security Center(NCSC) een extra waarschuwing afgegeven.

## NCSC

Vandaag laat het NCSC weten dat het patchen alleen effectief is als het onderliggende netwerk niet gecompromitteerd is. In alle gevallen adviseert het NCSC om ook na het nemen van mitigerende maatregelen, waaronder patches, te blijven monitoren en detectie toe te passen op de kwetsbaarheden. Onder de mitigerende maatregelen verstaat het NCSC de adviezen die Citrix gaf voor 9 januari 2020 om het risico van besmette systemen sterk te verminderen voordat er patches beschikbaar zouden komen. Het NCSC beschrijft twee scenario's. **Het eerste** gaat ervan uit dat de gebruiker de mitigerende maatregelen

heeft genomen. Dan kan men de patches gaan installeren. **Het tweede** gaat uit van de situatie dat de mitigerende maatregelen niet of pas na 9 januari 2020 zijn uitgevoerd. Dan kan men er gevoeglijk van uitgaan dat het computersysteem gecompromitteerd is. Dat vanwege het publiek bekend worden van aanvalsmogelijkheden(exploits). In dat geval moet men een herstelplan volgen.

## Herstelplan

In dat geval adviseert het NCSC  u om een herstelplan op te stellen, met daarin onder andere de volgende acties:

- *De gecompromitteerde systemen afkoppelen van het internet.*
- *De gecompromitteerde systemen aanbieden bij een partij voor forensisch onderzoek.*
- *De Citrix-systemen her-installeren en deze te voorzien van de mitigerende maatregelen en de patches zodra die beschikbaar zijn.*
- *Het implementeren van monitoringsmaatregelen om misbruik van de kwetsbaarheid te detecteren, zodat verdere compromittatie kan worden opgespoord. Vergeet hierbij niet de systemen die verbonden zijn geweest met de kwetsbare systemen gedurende het tijdsvenster van compromittatie.*

## Trage afkoppeling

De afgelopen week zagen we hoe in Nederland organisaties/bedrijven, instanties die de gewraakte Citrix ADC-servers gebruikten langzaam reageerden op het nieuws. Gaande de week koppelden grotere en kleinere gebruikers hun Citrix-servers af en konden medewerkers niet meer vanuit huis werken. Ook het NCSC droeg daar aan bij door het actief waarschuwen van niet-vitale infrastructuur niet tot haar takenpakket te beschouwen. Vanuit het bedrijfsleven kwam dan ook de roep om een breder mandaat voor het NCSC. Pa sop 17

januari kwam het NCSC met de oproep om Citrix-systemen uit te schakelen of mitigerende maatregelen te nemen.

## Lering

Wat leert dit alles ons? **Ten eerste** dat een gerenommeerd bedrijf als Citrix op zijn minst steken heeft laten vallen door het lek bekend te maken zonder dat er een patch was. In de **tweede plaats** dat het NCSC niet zo slagvaardig is als de naam doet vermoeden. In de **derde plaats** dat zeer veel inspanning om Citrix-gebruikers te waarschuwen gekomen is van cybersecurity-mensen van verschillende pluimage en deels werkend bij gerenommeerde bedrijven op dit terrein. Ik wil daarbij nogmaals het door hen opgerichte Dutch Institute of Vulnerability Disclosure(DIVD) noemen en het Nederlands Security Meldpunt (in oprichting). Die zagen wel waar de problemen lagen en hoe groot het probleem was. **Chapeau.**

W.J. Jongejan, 20 januari 2020

Afbeelding van Alexas_Fotos via Pixabay

---

# Systeembeheerders in de zorg: Wakker worden! Enorme kwetsbaarheid in Citrix Application Delivery Controller

**Vanaf half december 2019 is bekend dat er een forse kwetsbaarheid zit in de software van een aantal apparaten van de firma Citrix. Het gaat om de Citrix Application Delivery Controller (ADC). Die stond eerder bekend als de Netscaler ADC. Ook betreft het de Citrix Gateway die eerder bekend stond als de Netscaler Gateway. Door de kwetsbaarheid kan een niet geauthenticeerde indringer willekeurige commando's uitvoeren. Sinds 9 januari 2020 is bekend dat aanvallers actief gebruik proberen te maken van dit lek. Voor die tijd waren er nog geen kwaadwillige exploits gevonden.** Op 11 januari 202 werd duidelijk dat het kinderlijk eenvoudig was om van de kwetsbaarheid gebruik te maken. In Nederland zou het om ruim 700 via het publieke internet bereikbare Citrix ADC servers gaan. Daar zitten **naast overheidsinstellingen, meerdere zorginstellingen, zorgverzekeraars ook zorgaanbieders** bij. Een patch is vanaf 20 januari beschikbaar, maar systeembeheerders kunnen nu al maatregelen nemen.

## CVE-2019-19781

Kwetsbaarheden in hard- en software worden bijgehouden in een Amerikaanse database. Dat is de National Vulnerability Database(NVD) die de Common Vulnerabilities and Exposures(CVE) bijhoudt. De genoemde Citrix-kwetsbaarheid kreeg als nummer CVE-2019-19781. Deze informatie deelt men wereldwijd. Daarop kan dan geacteerd worden. De praktijk wijst helaas uit dat het handelen hiernaar door organisaties vaak niet de hoogste prioriteit heeft. Systeembeheerders kunnen of zelf laks zijn, of door de leiding afgehouden worden van alert reageren. Zulks op basis van het korte termijn denken dat de werking van de systemen voor de klanten niet door dit zeer noodzakelijk onderhoud onderbroken mag worden. Helaas is zeer recent duidelijk geworden dat zoiets tot grote narigheid leidt.

## Gevaar van niet reageren

Op 3 september 2019 schreef ik een artikel waarin ik refereerde aan een hot item: een kwetsbaarheid in kwetsbare Pulse Connect Secure SSL-VPNs in Nederlandse IP-adresruimte. Een aantal mensen uit de Nederlandse cybersecurity-scene die de gevaren ervan zagen, deden veel moeite om systeembeheerders van bedrijven te waarschuwen. Daar zaten overheidsinstellingen bij, maar ook instellingen en bedrijven van allerlei pluimage, ook uit de zorg. Heel recent bleek dat het grenswisselkantoor GWK Travelex getroffen was door ransomware. **Bij onderzoek kwamen zeven ungepatchte Pulse Connect servers aan het licht. En dat terwijl de softwarepatch beschikbaar was en men gewaarschuwd was.** Het toont genadeloos aan hoe kortzichtig het kan zijn om niet meteen in te grijpen. Nu zit GWK Travelex met een volledig versleuteld netwerk. Daarnaast is meer dan 5 GB aan persoonlijke data gestolen, waaronder geboortedata, social-security-nummers, betaalkaartgegevens en andere zaken. Voor het ontsleutelen van de data eisen de aanvallers 3 miljoen dollar.

## Welke soorten instellingen nu?

Tot nu toe zijn ruim 700 via het publieke internet bereikbare kwetsbare Citrix ADC servers bekend. Net zoals bij de Pulse Connect kwetsbaarheid zitten er bij het Citrix-gebeuren **veel zorgaanbieders bij. Ziekenhuizen, GGZ-instellingen (waaronder een verslavingskliniek), een paar zorgverzekeraars, en meerdere doelgroep-zorgaanbieders (bijv. ouderen). Uiteraard zijn er ook weer een aantal hits bij Rijksoverheid-systemen.** Hoewel de softwarepatch voor de Citrix-kwetsbaarheid nog niet voorhanden is kunnen systeembeheerders de configuratie van de Citrix ADC en andere hierboven genoemde apparaten wel zodanig wijzigen dat het gevaar substantieel minder is. Ook kan men voorbereidingen treffen om de binnenkort beschikbare patch te installeren. Op Nu.nl was op 13 januari 2020 hierover ook een item te zien.

## Dutch Institute of Vulnerability Disclosure

Juist voor dit soort situaties is zeer recent, in de herfst van 2019 het Dutch Institute of Vulnerability Disclosure(DIVD) opgericht. Het is een netwerk van cybersecurity-researchers, vrijwilligers die voornamelijk online werken. Er is geen fysiek kantoor . Bij kwetsbaarheden in hard- of software is gebleken dat het Nationaal Cyber Security Centrum(NCSC) zich eigenlijk voornamelijk richt op de overheid en vitale infrastructuur. Juist ten aanzien van acties richting een brede groep gebruikers in bedrijfsleven, dienstensector en non-profit-organisaties is gerichte actie nodig om kwetsbaarheden dringend onder de aandacht te brengen. Binnen DIVD is men gestart met het Nederlands Security Meldpunt (in oprichting). Het is een groep vrijwilligers, onderdeel van het DIVD, die het zich tot taak heeft gesteld eigenaren van Nederlandse netwerkblokken en websites te informeren over (cyber)security-zaken die bij het meldpunt gemeld worden. Over de Citrix-kwestie verscheen op 13 januari 2019 ook een bericht. Het zijn loffelijke initiatieven.

## Actie

Het is nu zaak dat systeembeheerders en cybersecurity-specialisten in de zorg in de eerste plaats nagaan of ze Citrix ADC apparaten in hun configuratie hebben staan en in de tweede plaats actie ondernemen om het gevaar te beperken en op scherp te staan als de beveiligingspatch zeer binnenkort beschikbaar is.

W.J. Jongejan, 14 januari 2020

Afbeelding van Sarah Richter via Pixabay