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