Casus Citrix Netscaler kwetsbaarheid juli 2025

Achtergrond

Donderdag 17 juli was uitgebreid in het nieuws dat het OM offline ging door ernstige zorgen over de beveiliging van de digitale werkomgeving. Op basis van een advies van het NCSC werden alle internetverbindingen afgesloten en werken op afstand was niet meer mogelijk. Het betreft een kwetsbaarheid in de Citrix NetScaler-software en het NCSC heeft signalen dat deze kwetsbaarheid actief wordt misbruikt. De minister J&V heeft met een brief de 2e kamer geinformeerd.

Vorige maand is een kwetsbaarheid in deze software gevonden (CVE-2025-5777 met een CVSS score van 9.3) en daarvan is op 18 juni een patch uitgebracht. De kwetsbaarheid kreeg de naam Citrixbleed 2 omdat het lijkt op een kwetsbaarheid uit 2023. Door een HTTP-POST request met een verkeerde inlogparameter te sturen naar een bepaald endpoint verwerkt de netscaler deze invoer onjuist en kunnen authenticatietokens en inloggegevens worden verkregen. Dit betekent dat je de authenticatiie en MFA potentieel bypassed. (ook wel out-of-bound read genoemd). Op 25 juni is een 2e patch uitgekomen. Beide keren heeft JIO de patch supersnel uitgevoerd. (binnen het uur)

Het NCSC en Citrix hebben vorige week IOC's en een script gedeeld waarmee organisaties kunnen testen of er sporen achtergebleven zijn die duiden dat een hacker toegang heeft gekregen. Ondanks dat we alles heel snel hebben gepatched zijn er sporen van een aanval gevonden: een verdachte file (binary) en een php webshell. In de logging is te zien dat er verkeer via die shell liep en dat dit is gestopt na het verwijderen van de shell.

Tijdlijn

- **18 juni 2025**: het NCSC geeft een alert dat de Netscaler een kwetsbaarheid heeft die actief wordt misbruikt. JIO had al op 17 juni deze kwetsbaarheid gepatched.
- **25 juni**: het NCSC komt met een 2e alert en Citrix komt met een 2e patch om 17.00u die JIO oind 18.00u heeft doorgevoerd op dezelfde dag
- **8 juli**: op basis van IOC's (hashes en IP addressen), gedeeld door het NCSC wordt een binary en een php webshell gevonden. Deze worden verwijderd.
- De timestamp van de binary staat op 17 juni, dat betekent dat deze al aanwezig was voor de eerste patch.
- **17 juli**: Ik word op de hoogte gesteld door 5.1 5.1.2e (SOC) en 5.1.2e dat zij bezig zijn met het reconstrueren van de aanval maar dat er problemen zijn met het verkrijgen van de nodige logfiles.
- **18 juli**: intern worden door SOC, Infra (teams 5.1.2e 5.1.2e en 5.1.2e 5.1.2e) en netwerk teams gekeken naar de kwetsbaarheid. Er is contact met NCSC, (die beheren de Netscalers) en het SOC JenV. Ook worden er vragen gesteld vanuit de opdrachtgevers. (m.n. 5.1.2e 5.1.2e stuurt een paar mails met vragen, maar ook de AP vraagt om informatie).
- **19 juli**: om 12 uur is een overleg met het NCSC over de situatie. Het NCSC adviseert om een partij in de arm te nemen die een 'compromise assessment' uitvoert om zo goed mogelijk ut te kunnen sluiten dat er geen attacker meer in het netwerk zit. Er zijn 3 partijen binnen de

raamovereenkomst met JenV (5.1.2f , 5.1.2f en). 5.1.2f wordt gebeld en om 14.15 wordt een intake-gesprek georganiseerd. Op basis van dit overleg wordt een actielijst opgesteld en gaan de technische mensen van JIO aan de slag. Om 16.45 wordt een terugkoppeling gehouden. De afspraak is om zondag 20 juli in Gouda verder te gaan . (en de technische mensen van JIO)

Overleggen

19-07-2025: 12.00 Overleg JIO – NCSC (online)

Aanwezig: 5.1.2e 5.1.2e , 5.1.2e 5.1.2e 5.1.2e , 5.1.2e 5.1.2e , 5.1.2e 5.5.1.2e , 6 mensen van NCSC (5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e)

5.1.2e geeft een overzicht van de tijdlijn en de acties die zijn uitgezet. In het SIEM van SOC JenV zijn hits gevonden opv de IOC's die zijn gedeeld, waaronder 3 netscalers van JIO. De events stoppen op 8 juli. 5.1.2e vraagt oh NCSC dit ook ziet, en dat wordt bevestigd.

Het NCSC vraagt of er al een IR partij is aangehaakt. Dit is nog niet het geval.

5.1.2e geeft aan dat de verkeerstromen in kaart moet brengen en de dat de FW gecheckt moet worden op IP adressen anders is geen correlatie mogelijk. Het lijkt nu alsof het alleen in de DMZ (bij) afspeelt.

NCSC geeft aan dat er echt een externe partij nodig is die een compromise assessment gaat uitvoeren. Op basis van de webshell moet gecontroleerd worden of er lateraal verkeer is geweest en/of anere persistence.

Het NCSC zal/kan informatie delen als deze beschikbaar is, maar heeft zelf ook informatiebehoefte. Welke partijen (opdrachtgevers) zijn betrokken, is er C2 verkeer gezien? Er zijn formele afspraken nodig over samenwerking en delen van informatie. (**actiepunt JIO om dit zsm op te pakken**)

NCSC: vraag wie moet aansluiten 5.1.2h (het beveiligde infokanaal waar informatie en bestanden worden gedeeld). 5.1.2e kan er al bij maar stuurt lijst met namen naar 5.1.2e

De discussie gaat over het afsluiten van internet. Het OM heeft dit gedaan na indicatie van compromise. Voor JIO zal eerst een onderzoek gedaan moet worden om dit te bevestigen/ uit te sluiten. Daarna zal samen met opdrachtgevers een risicoanalyse gemaakt moeten worden om dit wel/niet te doen.

NCSC: bereid het in ieder geval voor!

NCSC: hoe loopt de bestuurlijke lijn? Bij afwezigheid van 5.1.2e en 5.1.2e loopt dit via 5.1.2e 5.1.2e . Communicatie richting opdrachtgevers loopt formeel via 5.1.2e en nu in de praktijk via 5.1.2e en 5.1.2e.

Er moet ook nog een intern aanspreekpunt aan het NCSC gekoppeld worden. (**actie: uitzoeken wie, heb ik niet meer scherp**.... Denk 5.1.2e of 5.1.2e??)

Wie doet aangifte bij de politie? Vraag staat nog open... BVC of ook 5.1.2e (**actie, navraag**)

19-07-2025 13.00 nabespreking

Aanwezig: 5.1.2e 5.1.2e e , 5.1.2e 5.1.2e)

Welke partij gaan we inschakelen voor de compromise assessment? We bellen eerst met en kijken welke partij het eerst kan aanhaken. 5.1.2e 5.1.2e met 5.1.2e heeft contact met 5.1.2f maar had al aangegeven te kunnen aanhaken deze middag.

We gaan nog niet afsluiten, dat is pas de allerlaatste optie.

5.1.2e en 5.1.2e (nescaler team) zijn ook al op de hoogte en zullen aanhaken bij volgende gesprekken, evenals 5.1.2e 5.1.2e (netwerk)

We moeten 2 draaiboeken voorbereiden: loskoppelen van internet en communicatie.

19-07-2025 14:15 overleg 5.1.2f

Aanwezig: 5.1.2e 1 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1. 5.1.2e 5.1.2e 5.1.2e 5.1.2e, 5.1.2e, 5.1.2e (5.1.2f), 5.1.2e (5.1.2f), 5.1.2e (5.1.2f), 5.1.2e (5.1.2f). 5.1.2e (NCSC), 5.1.2e (NCSC)

2 onderwerp: opdracht compromise assessemnt en actielijst

5.1.2e geeft weer een overzicht en tijdlijn van gebeurtenissen

5.1.2f vraagt welke aanvullende onderzoeken/ actties we hebben gedaan of andere tooling hebben gebruikt om verdachte zaken te checken? 5.1.2e geeft aan geen andere tooling te hebben gebruikt en geen verdere verdachte acties te hebben gezien. Ook geen specifieke alerts. Na 8 juli is er geen verdachte activiteit door het SOC gesignaleerd.

5.1.2f vraagt zaken over infrasturctuur, bv wlke EDR we gebruiken etc. Ook hoeveel % aangesloten is en waar we zicht op hebben. 5.1.2h

5.1.2e

5.1.2h

5.1.2f 5.1.2h

5.1.2h

zijn er FW excepties, zijn die inzichtelijk? Dat moet worden uitgezocht, ook met hulp van . De FW bedienen meerdere organisaties. (vb DJI is ook voor FT&V)

Voor de scope van het onderzoek is het belangrijk om inzichtelijk te krijgen wat er achter de netscalers zit. Hoeveel netscalers zijn er? Totaal 5.1.2h .

Na een crash op 7 mei is in overleg met Citrix besloten om de netscalers te upgraden naar een nieuwe build.

5.1.2h

5.1.2e vraagt hoe om te gaan met de opdrachtomschrijving, hij vraagt ook om tijdlijnen en een rapport voor besluitvorming.

geeft aan dat ze in deze fase (bij mogelijke compromise) generiek support bieden: wat, hoe impact, waarom, sporen. Ipv veel tijd kwijt te zijn met scopebepaling willen ze meer actiegericht te werk gaan en minder planmatig.

5.1.2e zal de opdracht met formaliseren (**actie** 5.1.2e)

geeft aan dat ze ook een contactpersoon nodig hebben (ook hier weer 5.1.2e denk ik..ook gemist wat er is afgesproken)

5.1.2f we gaan aan de slag met de technische mensen, ze hebben informatie nodig. (actielijst wordt in de chat gedeeld, opvragen FW logging etc

NCSC geeft aan dat ze nu aan de zijlijn staan totdat het onderzoek is afgerond, maar ze zullen aanhaken als er aanvullende informatie bij hen of bij ons bekend is.

19-07 16:45 einde van de dag terugkoppeling

Aanwezig: medewerkers JIO (zelfde als eerder) en idem)

Er wordt nu hard gewerkt aan het opzoeken en leveren van de gevraagde data.

Zondag om 10 uur wordt in Gouda afgesproken om fysiek verder te gaan op aandringen van Dit is voor de beeldvorming en scope bepaling handiger met een BOB model en whiteboard dan via online overleggen.

Het netwerk is groot en complex , het zal even duren om dat te doorgonden en dat is makkelijker in een fysieke gezamelijke sessie.

Het pand moet geop[end worden, 5.1.2e heeft contact om dit te regelen

heeft een tool: 5.1.2h voor data collectie. Incident informatie wordt gedeeld via 5.1.2h

Er moeten ook nog opties worden uitgedacht over lange termijn onderzoek. (moet 5.1.2f een account krijgen in onze omgeving?)

5.1.2e geeft aan dat het lastig zal worden om bv alle FW data te uploaden, het is echt heel veel data. Het zou beter zijn als du9delijk is welke data daarvan nodig is. kan dat nog niet zeggen. De FW data gaan via .

Soc JIO krijgt ook toegang tot een dataset van SOC JenV om ook relaties te kunnen leggen met de netscalers van de opdrachtgevers. Zondag komt ook iemand 5.1.2e van SOC JenV naar gOuda.