Voorafgaand
Op de dag van publicatie van beide kwetsbaarheden (CVE2025-5777 17 juni, CVE2025-6543 25 juni) zijn de updates geïnstalleerd op Netscalers en zijn de mitigerende maatregelen zoals voorgeschreven door Citrix uitgevoerd op de aan het internet gekoppelde Netscalers. Voor beide kwetsbaarheden zijn op de opvolgende werkdagen (18 en 26 juni) dezelfde werkzaamheden uitgevoerd op de interne Netscalers. Citrix heeft bij de 2 patches die ze hebben uitgebreid ook gecommuniceerd dat er geen signalen van actief misbruik is geconstateerd.

8 mei - 26 mei 2025
Tijdens deze periode wordt instabiliteit ervaren op diverse Citrix Netscalers. Er is veelvuldig contact waarbij geheugendumps worden gedeeld met Citrix voor troubleshooting. Deze geheugendumps worden handmatig aangemaakt. Op 8 mei en 26 mei worden geheugendumps gedeeld met Citrix voor troubleshooting. De geheugendump van 8 mei bevat geen sporen van malafide activiteiten. In de geheugendump van 26 mei wordt echter een achterdeur (web shell) aangetroffen door Citrix.

26 mei 2025
Succesvolle toegang tot onze Netscaler met de zero-day exploit

18 juni 2025
Citrix brengt de eerste release uit voor het beveiligingslek
Dezelfde dag wordt deze patch geïnstalleerd op de buitenste Netscalers

19 juni 2025
De binnenste Netscalers worden voorzien van de beveligingspatch

25 juni 2025
Citrix brengt een tweede release uit voor het beveligingslek. De eerste patch bleek niet afdoende.
25 juni buitenste netscalers worden voorzien van deze beveiligingspatch 2

26 juni 2025
De binnenste Netscalers worden voorzien van de beveligingspatch 2

8 juli 2025
Op 8 juli wordt JIO op de hoogte gebracht door Citrix dat er een achterdeur is gevonden in de geheugendump die is gedeeld op 26 mei. Dit is een geheugendump van één Netscaler van DJI. Op advies van Citrix wordt deze Netscaler onderzocht en eventuele achterdeuren verwijderd. Er is toen nog geen incident response opgestart Er zijn mitigerende maatregelen genomen zoals het resetten van service accounts die actief zijn op de Netscalers en certificaten die door de Netscalers worden gebruikt t.b.v. authenticatie. De aangetroffen achterdeur is verwijderd en op basis van het huidige beeld van 5.1.2f zijn de Netscalers niet langer gecompromiteerd sinds 8 juli 2025. Nagaan waarom hebben wij geen aanvullende maatregelen toen opgestart?

moet je dit zeggen (wat je NIET gedaan hebt
5.1.2e 5.1.2e 5.1.2e
07/24/2025 13:28
Dit stond in de mail naar DJI

5.1.2e
07/24/2025 14:22

hoort niet bij 'Voorafgaand'
5.1.2e 5.1.2e
07/24/2025 13:31
Dit stond in de mail naar DJI

5.1.2e 5.1.2e
07/24/2025 14:22

Donderdag 17 juli 2025
Wij ontvingen het verzoek van NCSC om een script te draaien om na te gaan of er ongewenste activiteiten waren op de NetScaler. Er was door JIO tijdig gepatcht, maar de patch was niet voldoende en mogelijk waren de aanvallers al eerder op ons systeem binnengekomen. Gesprekken zijn mondeling gevoerd.
Advies: *We hebben nog geen advies aan onze opdrachtgevers kunnen geven, vanwege het feit dat we nog in de verkenningsfase zaten.*

Vrijdag 18 juli 2025
Wij hebben een tactisch gesprek gehad met NCSC, ook nav de ontwikkelingen van het OM, en hebben een advies gevraagd. Zij hebben ons geadviseerd een Private Incident Respons-partij in te schakelen, die een Compromised Assesment voor ons uit kunnen voeren. Gezien wij deze expertise niet in huis hebben. Het advies van het NCSC was om eerst het assesment uit te voeren, als daaruit blijkt dat de aanvaller verder was doorgedrongen dan de NetScaler dan zouden we wel aanvullende maatregelen moeten nemen, zoals (gedeeltelijk) afsluiten van internetverbindingen. afsluiten. De beheerafdelingen, SOC JIO SOC JenV en Solvinity hebben met elkaar de logging, op de NetScalers en op de andere systemen, gedeeld en nagelopen op ongewenste activiteiten op de servers. Hier is niets gevonden.

Aanvullende maatregelen moeten nemen, z
(gedeeltelijk) afsluiten van internet verbindi
5.1.2e 5.1.2e
07/24/2025 15:46

Advies: *We hebben een Private Incident Respons-partij ingeschakeld op advies van het NCSC. Ons advies aan onze opdrachtgevers is om vooralsnog niet offline te gaan, omdat er vanuit onderzoek naar onze monitoring nog geen ongewenste activiteiten hebben kunnen vinden.*

Zaterdag 19 juli 2025
We hebben een intake gesprek met de Private Incident Respons-partij gevoerd. Daarna hebben we alles in place gebracht om zondag op locatie verder te gaan met het assesment. Wij hebben onderzocht welke aanvullende gegevens de Private Incident Respons-partij nodig heeft om het onderzoek te doen. De meeting met de Private Incident Respons-partij was digitaal en heeft de eerste beelden van het incident en van de technische omgeving opgeleverd. De deelname hieraan was vanuit beheerafdelingen, SOC JIO, SOC J&V, Solvinity.

Advies: *De inzichten zijn nog niet gewijzigd, dus er is geen verandering in het advies.*

Zondag 20 juli 2025
In samenwerking met onze Private Incident Respons-partij zijn een drietal onderzoekssporen gedefinieerd die zich focussen op de verschillende aanvalsroutes die een aanvaller kan hebben genomen:

1. Netscaler-track: Verder onderzoek op gecompromitteerd systeem en vergelijkbare systemen die mogelijk ook kwetsbaar waren
2. Omliggende netwerktrack: Onderzoek van direct omliggende systemen die een aanvaller had kunnen aanvallen (binnenkant, beheerkant en buitenkant)
3. DWO/AD-track: Onderzoek op de digitale werkplek-omgeving (en active directory) die de aanvaller mogelijk had kunnen overnemen (DWO)

Belangrijke punten rondom de vraag of de digitale werkplek-omgeving (DWO) nog gebruikt kan worden:

- Het onderzoek van 5.1.2f is nog in opstartende fase
- Er is nog onvoldoende onderzoeksmateriaal geanalyseerd om uit te sluiten dat de aanvaller verder is gegaan dan het voorportaal dat toegang biedt tot de DWO
- De dekkingsgraad (van o.a. de DWO) van de security monitoring (EDR) moet verhoogd worden om actieve aanvallersactiviteit waar te nemen.

Vanwege bovenstaande punten, kan onze Private Incident Respons-partij nog geen eenduidig advies geven over deze vraag.

Advies: *Het advies is ongewijzigd omdat er geen bewijzen zijn dat er verder is doorgedrongen tot de beveiligde zone.*

Dit advies is gegeven naar aanleiding van een risicoanalyse van veiligheid vs business impact.
Business impact:

1. *De organisaties zijn voornamelijk mobiel ingericht, dit houdt in dat een groot deel van de medewerkers niet op locatie kunnen werken.*
2. *Medewerkers kunnen niet meer vanuit huis werken, waardoor enorme impact ontstaat op de primaire processen;*
3. *Servers waarop de "kritieke systemen" 5.1.2h 1.2h draaien zijn aangesloten op het SIEM. Daar zijn geen ongewenste activiteiten waargenomen.*

nagaan of er nog aanvullingen zijn op onderstaande punten, zeker op veiligheid

Veiligheid:

1. *Voorportaal ingericht DMZ (Demilitarised Zone). Deze voorziening is ingericht ter verdediging van de systemen. Er waren geen signalen dat er door de beveiligde zone heen is gekomen.*
2. *Extra bewaking vanuit het SOC naast de reeds regulier lopende acties*
3. *. Technische afstemming met direct betrokkenen van BVZ. De technische experts zijn vanaf zaterdag direct betrokken en hebben de tijdslijnen toegelicht, welke technische stappen er zijn gezet in overeenstemming met de adviezen vanuit CITRIX en NSCS, daarnaast is er diepgaande systeemkennis welke gedeeld is met de* Private Incident Respons-partij. De inhoudelijke gesprekken, analyses en verdieping is in continue samenwerking met de technische experts (netwerk en platform). Besproken is o.a.:

ik wil even checken met mail 5.1.2e

5.1.2e
07/24/2025 13:49

logging, crash reports, backup, config wijzigingen, duiding van netwerkontwerp, duiding van firewall opbouw

4. *De omgeving op netscalers was veilig, er is niets waargenomen. Zichtbaarheid moest wel vergroot worden omdat je niet alles kon zien.*
5. *We blijven open tot we wat vinden, onderzoek waar kan hacker naar toe*

Wij zitten dichtbij onze opdrachtgevers en het is, in het geven van een gedegen advies, van groot belang om ook de impact van de business voor onze opdrachtgevers hierin mee te nemen. Op hoofdlijnen kunnen we inschatten wat de impact is en wat het belang is om online te kunnen blijven. Het is gemakkelijk om te zeggen wij sluiten alle systemen af, echter is dan het middel erger dan de kwaal. Zolang wij geen signalen ontvangen dat ze verder zijn gekomen dan het voorportaal, dan weegt het belang van de business zwaarder dan het mogelijke beveiligingsrisico. Daarnaast is het niet in te schatten wanneer je weer online kan gaan, de aanvaller kan zich dan nog steeds stil houden op de servers en later weer actief worden. Deze afweging is besproken met de CIO's van de grootste opdrachtgevers.

Maandag 21 juli 2025
De 1e resultaten van het compromised assesment zijn gedeeld. Pentesters gestart met hun onderzoek?
Advies: *De inzichten zijn nog niet gewijzigd, dus er is geen verandering in het besluit.*

Dinsdag 22 juli 2025
Wachtwoordwijziging voorgesteld door DJI ➔ Meenemen in dit verhaal? Zou ik wel doen: 'eerste' of herhaald' verzoek om wachtwoordwijziging
Advies: *De inzichten zijn nog niet gewijzigd, dus er is geen verandering in het besluit.*

Woensdag 23 juli 2025
Er zijn nog geen aanwijzingen vanuit het compromised assesment dat ze verder doorgedrongen zijn in de beveiligde zone. Tevens waren ze in staat om de sporen van de ongewenste activiteit uit de NetScalers te bekijken. Een deel van de periode die gelogd is, is nu onderzocht en ook daar zijn geen aanwijzingen dat ze daadwerkelijk verder zijn gekomen.
Advies: *De inzichten zijn nog niet gewijzigd, dus er is geen verandering in het besluit.*

Donderdag 24 juli 2025
De samenwerking met NCSC, team High Tech Crime van de Nationale Politie en CERT EU begint zijn vruchten af te werpen. Er zijn meerdere overheidsinstanties geraakt 5.1.2h,5.1.2i

5.1.2h,5.1.2i

5.1.2h,5.1.2i De tijdlijnen in de gedeelde informatie zijn in lijn met die van JIO. Alle getroffen organisaties zien dezelfde tijden en aanvalspartonen. 5.1.2h

5.1.2h

Achtergrond bij de genomen risicoanalyse op veiligheid:
Op 8 mei hadden we het volgende in place:

- 5.1.2h

Om de zichtbaarheid op onze omgeving te vergroten wordt er momenteel gewerkt aan de volgende acties:

- 5.1.2h
- Uitbreiden toezicht/monitoring op de Domain Controllers (EDR naast de al in Siem opgenomen eventlogging): Technische test vinden nu plaats, vanaf 25/7 gereed;
- Installeren 5.1.2h agents op de DWO (EDR naast de al in Siem opgenomen eventlogging); Technische tests vinden nu plaats in de test omgeving.

Wachtwoorden

- Als mitigerende maatregel aanpassen wachtwoorden op beheeraccounts