To: 5.1.2e 5.1.2e [5.1.2e @dji.minjus.nl]
Cc: 5.1.2e 5.1.2e @dji.minjus.nl]; 5.1.2e 5.1.2e [5.1.2e @jio.nl]
From: 5.1.2e
Sent: Mon 7/21/2025 9:08:04 AM
Subject: RE: Update 20-07-2025: Verzoek om technisch onderzoek Citrix ADC Netscaler kwetsbaarheden
Received: Mon 7/21/2025 9:08:04 AM

Beste 5.1.2e ,
Zoals afgesproken hierbij nadere informatie omtrent de kwetsbaarheid op de Netscaler.
Status bericht:

- ∀ Patch is in Juni geinstalleerd
- ∀ Controles iom Citrix hebben begin Juli plaatsgevonden, waarbij een Web shell gevonden is. Deze zijn verwijderd in overleg met Citrix.
- ∀ We zien alleen verkregen toegang tot de voorportaal bij Solvinity. We hebben nog geen aanwijzingen van sporen op de Netscaler in ons DC (Onderzoek loopt nog)
- ∀ We hebben geconstateerd dat er een kans is dat al langere tijd toegang op de netscaler is geweest
- ∀ We hebben geconstateerd dat IOC na 8 juli niet meer actief zijn geweest
- ∀ 5.1.2f is gevraagd om nader forensich onderzoek te doen
- ∀ De onderzoeks paden zijn gedefinieerd en de benodigde log data is/wordt verzameld. Vandaag zal 5.1.2f de nodige analyses opstarten en uitvoeren
- ∀ De scope is momenteel nog binnen de DWO omgeving, afhankelijk van de onderzoeks resultaten zal deze scope bijgesteld worden
- ∀ JIO kijkt samen met 5.1.2f naar mogelijke handelings perspectieven, maar deze zijn nu nog niet concreet genoeg om te delen
- ∀ Bij het onderzoek zijn SOC JenV en Solvinity nauw betrokken omdat met name de log data van Solvinity onderdeel is van het huidige onderzoek

Rond 13:00 zullen we een sessie hebben met de CISO's van opdrachtgevers
Ik verwacht vanmiddag of morgenochtend een nauwkeuriger beeld te hebben op het handelings perspectief.
Met vriendelijke groet,
5.1.2e 5.1.2e

.....
Directie Implementatie en Dienstverlening (ID)
Justitiële ICT Organisatie
Ministerie van Justitie en Veiligheid
Stavorenweg 3 | 2803 PT | Gouda | 5.1.2e
Laagbouw Postbus 850 | 2800 AW | Gouda
.....
T
F 5.1.2e
M 5.1.2e
Email: 5.1.2e @jio.nl
https://www.justitieleictorganisatie.nl
Volg ons ook op:



Van: 5.1.2e , 5.1.2e 5.1.2e
Verzonden: zondag 20 juli 2025 22:41
Aan: 5.1.2e 5.1.2e @dji.minjus.nl>; 5.1.2e : 5.1.2e @dji.minjus.nl>; 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>
CC: 5.1.2e 5.1.2e 2e < 5.1.2e @dji.minjus.nl>; 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e , 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>
Onderwerp: RE: Update 20-07-2025: Verzoek om technisch onderzoek Citrix ADC Netscaler kwetsbaarheden
Beste Collega,
Het forensisch onderzoek loopt nog en wordt morgen (21/07) gecontinueerd in Gouda.
Er is nog onvoldoende onderzoeksmateriaal om uit te sluiten dat de aanvaller verder is gegaan dan het voorportaal dat toegang biedt tot de werkplek. Dit op basis van de huidige informatie

Dagelijks zullen wij u informeren over de voortgang.
Met vriendelijke groet,

5.1.2e 5.1.2e

.....

Directie Implementatie en Dienstverlening (ID)
Justitiële ICT Organisatie
Ministerie van Justitie en Veiligheid
Stavorenweg 3 | 2803 PT | Gouda | 5.1.2e
Laagbouw Postbus 850 | 2800 AW | Gouda

.....

T 5.1.2e
F
M 5.1.2e
Email: 5.1.2e @jio.nl
https://www.justitieleictorganisatie.nl
Volg ons ook op:



Van: 5.1.2e , 5.1.2 5.1.2e
Verzonden: zaterdag 19 juli 2025 18:44
Aan: 5.1.2e 5.1.2e @dji.minjus.nl>; 5.1.2e 5.1.2e @dji.minjus.nl>; 5.1.2e 5.1.2e
< 5.1.2e @dji.minjus.nl>; 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>
CC: 5.1.2e 5. 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e
< 5.1.2e @dji.minjus.nl>; 5.1.2e , 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>
Onderwerp: RE: Update 19-07-2025: Verzoek om technisch onderzoek Citrix ADC Netscaler kwetsbaarheden

Beste Collega,
Het forensich onderzoek loopt nog door. Vandaag is 5.1.2f gevraagd om een compromised assessment uit te voeren. Hiervoor zijn vandaag de eerste sessies geweest, doel hiervan is om vast te stellen in welke mate misbruik heeft plaatsgevonden
Morgen gaat het onderzoek vervolgd worden in Gouda. Zo gauw ik weer relevante informatie heb zal ik deze communiceren.
Met vriendelijke groet,

5.1.2e

.....

Directie Implementatie en Dienstverlening (ID)
Justitiële ICT Organisatie
Ministerie van Justitie en Veiligheid
Stavorenweg 3 | 2803 PT | Gouda | 5.1.2e
Laagbouw Postbus 850 | 2800 AW | Gouda

.....

T 5.1.2e
F
M 5.1.2e
Email: 5.1.2e @jio.nl
https://www.justitieleictorganisatie.nl
Volg ons ook op:



Van: 5.1.2e , 5.1.2e 5.1.2e
Verzonden: vrijdag 18 juli 2025 23:09
Aan: 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e 5.1.2e
< 5.1.2e @dji.minjus.nl>; 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>
CC: 5.1.2e 5. 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e , 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e , 5.1.2e
< 5.1.2e @dji.minjus.nl>; 5.1.2e : 5.1.2e @dji.minjus.nl>; 5.1.2e , 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>

Onderwerp: Update 18-07-2025: Verzoek om technisch onderzoek Citrix ADC Netscaler kwetsbaarheden

Beste Collega,

Hierbij de laatste update van vandaag over de voortgang m.b.t. de kwetsbaarheid op onze Netscalers. Voortgang in geel

- Er is op dit onderwerp inmiddels ook een uitvraag aan ons gestuurd vanuit CIO Rijk. Neem deze vraagstelling mee als uitbreiding op mijn verzoek. Ook op tijdsverloop tussen eerste bekendmaking van de kwetsbaarheid (de betrokken CVE's) en het doorvoeren van security updates in verschillende onderdelen binnen de JIO-infrastructuur.
  - × IS reeds beantwoord voor DJI, in principe geldt deze beantwoording voor alle opdrachtgevers van Justitiele ICT Organisatie
- Het is voor DJI noodzakelijk om zo snel als mogelijk onzekerheid omtrent eventueel misbruik (ondanks vroegtijdig patchen) te kunnen wegnemen, danwel vervolgactie te kunnen nemen als anders blijkt. DJI vraagt JIO daarom om werkzaamheden voor technisch onderzoek ook dit weekeinde te laten doorlopen voor tenminste de internet gerichte Netscaler systemen waar deze kwetsbaarheid op aanwezig is geweest.
  - × Lopende het forensisch onderzoek met onze specialisten, NCSC, Solvinity en SOC JenV zijn we nog niet in staat om hier antwoord op te geven. Het onderzoek zal gecontinueerd worden gedurende het weekend.
  - ∀ DJI wil geïnformeerd worden over bevindingen van het technisch onderzoek. Terugkoppeling graag aan mij en 5.1.2e en aan 5.1.2e 5.1.2e en onze functionele IB Mailbox in cc.
  - Ik wil tenminste weten:
    - JIO heeft ons eind juni via de gebruikelijke lijn geïnformeerd dat een spoedpatch voor deze kwetsbaarheden is doorgevoerd. Dit heeft plaatsgehad op 25 en 26 juni. Is als onderdeel daarvan, of kort daarop, ook technisch onderzoek gepleegd op de op dat moment beschikbare Indicators Of Compromise?
  - × Technisch zijn alle Netscalers voorzien van de benodigde patches en zijn controles uitgevoerd op basis van instructies van NCSC en Citrix
    - Kan zich in onze omgeving hebben voorgedaan dat (kwetsbare) sessies nog na het patchen op de machines instant zijn gebleven, waardoor het risico op dat moment nog niet volledig gemitigeerd was? Zo ja, over welke periode is dit het geval geweest? Is nog in onderzoek met medewerking van NCSC
  - × Sessies via de Netscaler zijn tijdens de technisch controles afgebroken, hierbij is ook niet vastgesteld dat misbruik is gemaakt van de kwetsbaarheid op andere componenten die via de Netscaler te bereikt kunnen worden. Dit zal verder onderzocht worden binnen het forensisch onderzoek wat nog in behandeling is
    - Terugkoppeling of er op basis van de gehele set nu bekende Indicators Of Compromise in het technisch onderzoek sporen zijn van (mogelijk) misbruik. En zo ja advies voor verder handelingsperspectief voor DJI.
  - × Is nog onderdeel van het forensisch onderzoek, wij hebben de IOC's zoals aangeven na de patchronde teruggevonden in de firewall, echter nog geen aanwijzingen van misbruik
    - Kan JIO aan ons bevestigen dat alle relevante nu bekende IOC's bij deze kwetsbaarheid zijn opgenomen in de SIEM voorziening voor aanvalsdetectie?
  - × De IOC zijn opgenomen in de SIEM bij SOC JenV zodat ze zo vroeg mogelijk in de keten worden waargenomen. SOC Justitiele ICT Organisatie heeft hier ook inzage in en gebruikte deze informatie voor nadere analyse

Met vriendelijke groet,

5.1.2e 5.1.2e 5.1.2e

.....

Directie Implementatie en Dienstverlening (ID)
Justitiële ICT Organisatie
Ministerie van Justitie en Veiligheid
Stavorenweg 3 | 2803 PT | Gouda | 5.1.2e
Laagbouw Postbus 850 | 2800 AW | Gouda

.....

T 5.1.2e
F
M 5.1.2e
Email: 5.1.2e @jio.nl
https://www.justitieleictorganisatie.nl
Volg ons ook op:



Van: 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>
Verzonden: vrijdag 18 juli 2025 15:35
Aan: 5. 5.1.2e < 5.1.2e @dji.minjus.nl>

CC: 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e < 5.1.2e @dtv.minvenj.nl>; 5.1.2e , 5.1.2e . 5.1.2e < 5.1.2e @justis.nl> 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e , 5.1.2e.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl> 5.1.2e < 5.1.2e @dji.minjus.nl>

Onderwerp: RE: Verzoek om technisch onderzoek Citrix ADC Netscaler kwetsbaarheden

Hi 5.1.2e

Een correctie en aanvulling bij mijn voorgaand bericht.

Correctie:

In vorig bericht schreef ik dat patches op de systemen op **25 en 26 juni** zijn doorgevoerd. Dit is niet volledig en daarom niet juist. Patches zijn op de verschillende systemen door JIO gefaseerd doorgevoerd. Volgens onze informatie zijn de eerste (internet facing) Netscalers in onze omgeving door JIO reeds van updates voorzien op **17 juni**. Er zijn daarna meerdere patch-momenten geweest om het volledig in het landschap door te voeren.

Aanvulling:

- Er is op dit onderwerp inmiddels ook een uitvraag aan ons gestuurd vanuit CIO Rijk. Neem deze vraagstelling mee als uitbreiding op mijn verzoek. Ook op tijdsverloop tussen eerste bekendmaking van de kwetsbaarheid (de betrokken CVE's) en het doorvoeren van security updates in verschillende onderdelen binnen de JIO-infrastructuur.
- Het is voor DJI noodzakelijk om zo snel als mogelijk onzekerheid omtrent eventueel misbruik (ondanks vroegtijdig patchen) te kunnen wegnemen, danwel vervolgactie te kunnen nemen als anders blijkt. DJI vraagt JIO daarom om werkzaamheden voor technisch onderzoek ook dit weekeinde te laten doorlopen voor tenminste de internet gerichte Netscaler systemen waar deze kwetsbaarheid op aanwezig is geweest.

Ik ben, ook gedurende het weekeinde, telefonisch bereikbaar voor afstemming als de situatie daarom vraagt.

Vriendelijke groeten,

5.1.2e 5.1.2e

5.1.2e

.....

Directie Informatievoorziening | CIO-Office
Dienst Justitiële Inrichtingen
Ministerie van Justitie en Veiligheid
Turfmarkt 147 | 2511 DP | Den Haag

.....

5.1.2e
5.1.2e @dji.minjus.nl

Van: 5.1.2e 5.1.2e
Verzonden: vrijdag 18 juli 2025 13:31
Aan: 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>
CC: 5.1.2e 2 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e e 5.1.2e < 5.1.2e @dtv.minvenj.nl>; 5.1.2e , 5.1.2e < 5.1.2e @justis.nl>; 5. 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e 5.1.2e 2e < 5.1.2e @dji.minjus.nl>; 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e < 5.1.2e @dji.minjus.nl>

Onderwerp: Verzoek om technisch onderzoek Citrix ADC Netscaler kwetsbaarheden

Urgentie: Hoog

Beste 5.1.2e

Zoals eerder vanmiddag kort telefonisch besproken in dit bericht een verzoek omtrent NCSC-advies bij eerdere Citrix kwetsbaarheden. NCSC heeft een update gepubliceerd bij een recente H/H kwetsbaarheid in Citrix Netscaler software. In de update is een bijgesteld handelingsperspectief meegegeven.

https://advisories.ncsc.nl/advisory?id=NCSC-2025-0196

De hoofdelementen hierin:

Er zijn situaties dat een betreffend systeem nog vatbaar kan zijn voor misbruik nadat gepatcht is. En naar aanleiding van nieuwe informatie en ontwikkelingen rond constateringen van misbruik zijn er nieuwe Indicators of Compromise (IOC's) bekend gesteld. Het NCSC adviseert naar aanleiding daarvan **alle** organisaties die NetScaler ADC of Netscaler Gateway gebruiken om technisch onderzoek te doen naar mogelijk misbruik.

Bij deze verzoek ik namens DJI aan JIO om conform het advies van NCSC technisch onderzoek te plegen op sporen van eventuele compromittatie van de (alle) Netscalers in de infrastructuur van JIO voor dienstverlening aan DJI. Dit op basis van de gehele set van nu bekende indicatoren en aanvullende informatie in de NCSC Advisory. En daarbij om opvolging van alle overige aanwijzingen in

het geadviseerd handelingsperspectief uit het NCSC advies, voor zover dat op basis van uitkomsten van het onderzoek nodig blijkt.

- ∀ Laat dit onderzoek onmiddellijk starten, als dat niet al is aangevangen op initiatief van JIO zelf. Dit is nodig om zo snel als mogelijk te weten of er onverhoopt bij ons toch risico is op misbruik.
- ∀ DJI wil geïnformeerd worden over bevindingen van het technisch onderzoek. Terugkoppeling graag aan mij en 5.1.2e en aan 5.1.2e 5.1.2e en onze functionele IB Mailbox in cc.

Ik wil tenminste weten:

- JIO heeft ons eind juni via de gebruikelijke lijn geïnformeerd dat een spoedpatch voor deze kwetsbaarheden is doorgevoerd. Dit heeft plaatsgehad op 25 en 26 juni. Is als onderdeel daarvan, of kort daarop, ook technisch onderzoek gepleegd op de op dat moment beschikbare Indicators Of Compromise?
- Kan zich in onze omgeving hebben voorgedaan dat (kwetsbare) sessies nog na het patchen op de machines instant zijn gebleven, waardoor het risico op dat moment nog niet volledig gemitigeerd was? Zo ja, over welke periode is dit het geval geweest?
- Terugkoppeling of er op basis van de gehele set nu bekende Indicators Of Compromise in het technisch onderzoek sporen zijn van (mogelijk) misbruik. En zo ja advies voor verder handelingsperspectief voor DJI.
- Kan JIO aan ons bevestigen dat alle relevante nu bekende IOC's bij deze kwetsbaarheid zijn opgenomen in de SIEM voorziening voor aanvalsdetectie?

Ik hoor graag zo spoedig als mogelijk het resultaat. Koppel natuurlijk ook gedeeltelijke beantwoording en onderzoeksresultaat terug zodra daar aanleiding voor is.

Vriendelijke groeten,

5.1.2e 5.1.2e

5.1.2e

Directie Informatievoorziening | CIO-Office
Dienst Justitiële Inrichtingen
Ministerie van Justitie en Veiligheid
Turfmarkt 147 | 2511 DP | Den Haag

M 5.1.2e
E 5.1.2e @dji.minjus.nl