To: 5.1.2e , 5.1.2e [5.1.2e @dtenv.nl]; 5.1.2e [5.1.2e @jio.nl]; 5.1.2e , 5.1.2e [5.1.2e @dtenv.nl]; 5.1.2e 5.1.2e [5.1.2e @dtenv.nl]
Cc: 5.1.2e , 5.1.2e . 5.1.2e 5.1.2e @justis.nl]; 5.1.2e 5 5.1.2e 5.1.2e @jio.nl]; 5.1.2e , 5.1.2e [5.1.2e @dji.minjus.nl]; 5.1.2i 5.1.2i @dji.minjus.nl]; 5.1.2i 5.1.2i 5.1.2i @dtenv.nl]
From: 5.1.2e , 5.1.2e .2e
Sent: Fri 7/18/2025 9:20:18 PM
Subject: Update 18-07-2025 : Reactie DTenV: Verzoek om technisch onderzoek Citrix ADC Netscaler kwetsbaarheden
Received: Fri 7/18/2025 9:20:18 PM

Beste Collega,
Laatste update mbt de kwetsbaarheid van de Netscalers.
Technische controle en de patches zijn door Justitiele ICT Organisatie in Juni uitgevoerd conform aangeven door NCSC.
Forensisch onderzoek zal gedurende het weekend gecontinueerd worden. Onderzoek wordt uitgevoerd door Specialisten van Justitiele ICT Organisatie, NCSC, Solvinity en SOC JenV. Misbruik is tot op heden niet vastgesteld.
De SIEM omgeving is voorzien van de IOC's voor zover deze nu bekend zijn.
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 @dtv.minvenj.nl>
Verzonden: vrijdag 18 juli 2025 14:06
Aan: 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e < 5.1.2e @jio.nl>; 5.1.2e , 5.1.2e < 5.1.2e @dtv.minvenj.nl>; 5.1.2e , 5.1.2e < 5.1.2e @dtv.minvenj.nl>
CC: 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 < 5.1.2e @dji.minjus.nl>; 5.1.2e , 5.1.2e . - 5.1.2e @justis.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>; 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2i < 5.1.2i @dji.minjus.nl> 5.1.2i 5.1.2i @dtv.minvenj.nl>; 5.1.2e , 5.1.2e < 5.1.2e @dtv.minvenj.nl>
Onderwerp: Reactie DTenV: Verzoek om technisch onderzoek Citrix ADC Netscaler kwetsbaarheden

Goedemiddag 5.1.2e ,
Dank voor het delen van jouw bericht met de DTenV. Dit wordt zeer gewaardeerd!
@ 5.1.2e , wij onderkennen wat er hieronder door DJI is beschreven en wij sluiten aan bij het geformuleerde verzoek van 5.1.2e .
buiten verzoek vandaar dat ik 5.1.2e en 5.1.2e 5.1.2e 5.1.2e inkopieer, zodat zij van het bovenstaande op de hoogte zijn. Graag svp bij alle e-mail correspondentie over dit onderwerp na vandaag 5.1.2e en 5.1.2e meenemen. Gaat dit lukken?
Hartelijke groet,

5.1.2e 5.1.2e

.....
Afdeling Bedrijfsvoering | Team Business Information Technology (BIT)
Dienst Terugkeer en Vertrek
Ministerie van Asiel en Migratie
Ministerie van Justitie en Veiligheid

Rijnstraat 8 | 2515 XP | Den Haag
Postbus 164 | 2501 CD | Den Haag
BIT Informatiebeveiliging: 5.1.2i @dtv.minvenj.nl
DTenV Secretariaat ICT: 5.1.2e @dtv.minvenj.nl
Webex-ruimte: 5.1.2i
.....
M +31 (5.1.2e
5.1.2e @dtv.minvenj.nl
http://www.dienstterugkeerenvertrek.nl
.....
Samenwerken aan respectvolle terugkeer
.....
Ik ben woensdag niet aanwezig op kantoor.
CC-berichten worden automatisch in een aparte map geplaatst en niet regelmatig gelezen.

Van: 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>
Verzonden: vrijdag 18 juli 2025 13:31
Aan: 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>
CC: 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 < 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 < 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>; GOUPU Informatiebeveiliging < 5.1.2i @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 o 5.1.2i re 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