To: 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 @dji.minjus.nl]; 5.1.2e , 5.1.2e [5.1.2e @dji.minjus.nl]; 5.1.2e , 5.1.2e (5.1.2e @jio.nl]
From: 5.1.2e , 5.1.2e
Sent: Tue 7/22/2025 5:35:48 PM
Subject: RE: Update Netscaler kwetsbaarheid
Received: Tue 7/22/2025 5:35:54 PM

Hoi 5.1.2e ,
Sinds vandaag zijn het NCSC en het Team High Tech Crime van de politie ook formeel aangehaakt.
FF toevoegen aan de onderstaande zin.
Daarom zijn wij, samen met 5.1.2f , Solvinity en SOC JenV, een forensisch onderzoek gestart.
Verder akkoord.
Groet,
5.1.2e

Van: 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>
Verzonden: dinsdag 22 juli 2025 19:20
Aan: 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 @dji.minjus.nl>; 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e , 5.1.2e < 5.1.2e @jio.nl>
Onderwerp: Re: Update Netscaler kwetsbaarheid

Domain controllers zonder DWO erachter bij punt 2 helemaal onderaan
DWO wordt al bij punt 3 genoemd
Verder akkoord

Van: " 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>
Datum: dinsdag 22 juli 2025 om 19:02:31
Aan: " 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 @dji.minjus.nl>, " 5.1.2e , 5.1.2e < 5.1.2e @jio.nl>, " 5.1.2e , 5.1.2e " < 5.1.2e @dji.minjus.nl>
Onderwerp: Update Netscaler kwetsbaarheid

Checken jullie even of dit de lading dekt qua informatie ? (zowel voor CIO's als CISO's)
Collega's,
Zoals eerder al met jullie gedeeld heeft via een kwetsbaarheid in de Citrix Netscaler een onbekende aanvaller zich toegang verschaft tot een voorportaal van onze digitale werkplek omgeving. Het voorportaal is belangrijk om gebruikers toegang te geven tot de kantoorautomatisering. Daarom zijn wij, samen met 5.1.2f , Solvinity en SOC JenV, een forensisch onderzoek gestart. Hiervoor zijn ism met onze externe leverancier (5.1.2f) 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 netwerk track: 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 die de aanvaller mogelijk had kunnen overnemen (DWO)

Statusupdate 22-7:
In het reguliere overleg met de CISO's van onze opdrachtgevers is de behoefte uitgesproken dat men meer focus wil hebben op handelingsperspectieven. Dit is meegenomen in de End of Day van ons directieteam waarbij de formele actie is uitgezet om de handelingsperspectieven rondom de kroonjuwelen samen met opdrachtgevers verder versneld uit te werken. Rondom aanvalsroute 2 zijn onze pen-testers ingezet om deze aanvalsroute versneld te verkennen zodat we daarmee meer inzicht krijgen in de potentiele vervolgpaden voor het forensisch onderzoek.

Voorlopige bevindingen:

1. De initiële toegang vond plaats rond 26 mei 2025 03:56 UTC (05:56 uur Nederlandse tijd)
2. Installeren van patches vond plaats rond 17 en 25 juni, kort na publicatie van de kwetsbaarheden
3. Op 7 juli meldt Citrix de vondst van een backdoor webshell in de op 26 mei opgestuurde crash dumps

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

5.1.2i
5.1.2h

Er zijn vooralsnog nog geen concrete aanwijzingen dat deze aanvaller verder dan het voorportaal is weten te komen. Op dit moment zijn al onze systemen online, waardoor dit geen impact heeft op onze dienstverlening.
Met vriendelijke groet,
5.1.2e
5.1.2e

Justitiële ICT Organisatie
Ministerie van Justitie en Veiligheid
Stavorenweg 3 | 2803 PT | Gouda
Postbus 850 | 2800 AW | Gouda
Managementondersteuner: 5.1.2e | 5.1.2e @jio.nl | T 5.1.2e | 5.1.2e
M 5.1.2e
5.1.2e @jio.nl
https://www.justitieleictorganisatie.nl
Volg ons ook op: