To: 5.1.2e , 5.1.2e [5.1.2e @jio.nl]
From: 5.1.2e , 5.1.2e
Sent: Wed 7/30/2025 9:32:33 AM
Subject: Re: [TLP:STRICT-AMBER] Update 4: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway
Received: Wed 7/30/2025 9:32:34 AM

Top thx

From: " 5.1.2e , 5.1.2e " < 5.1.2e @dji.minjus.nl>
Date: Wednesday, 30 July 2025 at 11:01:51
To: " 5.1.2e , 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>
Subject: RE: [TLP:STRICT-AMBER] Update 4: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway

Goedemorgen 5.1.2e,
Zoals ik vanmorgen telefonisch al zei: we hebben de IOC op alle Netscalers gedraaid (internet facing en in het datacenter) en de controles ook herhaald en uitgebreid als hiervoor berichten kwamen.
Met vriendelijke groet,

5.1.2e 5.1.2e 5.1.2e
5.1.2e

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

Mail die ik ontvang als CC bewaar ik als referentie, hierop onderneem ik geen actie.
Denk aan het milieu: is uitprinten wel nodig?



Van: 5.1.2e , 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>
Verzonden: dinsdag 29 juli 2025 19:09
Aan: 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>
Onderwerp: FW: [TLP:STRICT-AMBER] Update 4: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway
Beste 5.1.2e,
Zie onderstaand. Kun / wil jij bevestigen dat dit ook zo wordt uitgevoerd. Zover wij weten wel, maar je weet het nooit.
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: dinsdag 29 juli 2025 18:53
Aan: 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.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 @dji.minjus.nl>; 5.1.2e , 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 .1.2e < 5.1.2e @dtv.minvenj.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 @dtv.minvenj.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 @dtv.minvenj.nl>; 5.1.2e @minjenv.nl' < 5.1.2e @minjenv.nl>; 5.1.2e @rvdk.nl' < 5.1.2e @rvdk.nl>; 5.1.2e , 5.1.2e 5.1.2e < 5.1.2e @justis.nl>; 5.1.2e @minjenv.nl' < 5.1.2e @minjenv.nl>; 5.1.2e @autoriteitpersoonsgegevens.nl' < 5.1.2e @autoriteitpersoonsgegevens.nl>
Onderwerp: RE: [TLP:STRICT-AMBER] Update 4: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway
Beste 5.1.2e ,
Wij volgen de instructies vanuit het NCSC en Citrix op aangaande de genoemde kwetsbaarheden. In scope zijn alle netscalers voor dit soort informatie.
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)
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 @dji.minjus.nl>
Verzonden: maandag 28 juli 2025 19:44
Aan: 5.1.2e , 5.1.2e5.1.2e < 5.1.2e @dji.minjus.nl>
CC: 5.1.2e , 5.1.2 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>; 5.1.2i 5.1.2i @dji.minjus.nl>
Onderwerp: FW: [TLP:STRICT-AMBER] Update 4: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway
Hallo 5.1.2e,
Ik neem aan dat JIO onderstaande nieuwe controles meeneemt in het lopend onderzoek. Niet alleen voor de NetScaler waarvan bekend is dat die geraakt is, maar ook alle overige NetScaler instances. Kun je dat bevestigen?

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

Van: 5.1.2i @lists.ncsc.nl>
Verzonden: maandag 28 juli 2025 17:59
Aan: 5.1.2i @ncsc.nl>
Onderwerp: [Rijks-isac] [TLP:STRICT-AMBER] Update 4: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512
[TLP:AMBER+STRICT]
** ENGLISH VERSION BELOW **
Best NCSC partner,
Het NCSC adviseert om zelf handmatig forensisch onderzoek te doen naar de Citrix Netscaler casus en dit zo spoedig mogelijk uit te voeren. Uit ons onderzoek blijkt dat sporen van compromitatie mogelijk al snel gewist worden. Hieronder lees je hoe je zelf onderzoek kan doen kan. Als dit onderzoek niet tijdig wordt uitgevoerd is de kans groter dat op gecompromiteerde systemen de actor onopgemerkt toegang behoudt.
Het uitbuiten van de kwetsbaarheid kan leiden tot coredump bestanden. Deze bestanden zijn vindbaar op een Citrix Netscaler oplossing onder het pad 5.1.2h Mochten hieronder een aantal genummerde submappen met 5.1.2h bestanden in staan, dan verzoeken wij deze aan te leveren aan het NCSC voor nadere analyse. Data kan worden geüpload via https://securetransfer.rijkscloud.nl/versturen, t.a.v 5.1.2i @ncsc.nl
Het NCSC is in staat bestanden te onderzoeken op bekende kenmerken behorende tot deze campagne. Een eerste triage kan worden uitgevoerd door

buiten verzoek

Bij het aantreffen van een of meer van de bovengenoemde IOC's is vervolgonderzoek nodig om vast te stellen of er daadwerkelijk compromitatie heeft plaatsgevonden. Neem in dat geval contact op met cert@ncsc.nl voor verdere ondersteuning.
** ENGLISH VERSION **
Dear NCSC partner,
The NCSC advises to perform manual forensic investigation into the Cirtix Netscaler case, and to perform this as soon as possible. Our investigation shows that signs of compromise can be deleted before they are noticed. Below we explain how to investigate. Not performing this investigation in a timely matter could result in the actor retaining unnoticed access to compromised systems.
Exploitation of the vulnerability can result in the creation of coredump files. These files can be found on a Citrix Netscaler instance in the path: 5.1.2h If any numbered sub directories are found which contain .gz

files, we would like to receive these files for further investigation.
These files can be uploaded to:
https://securetransfer.rijkscloud.nl/versturen attn. 5.1.2i @ncsc.nl
Our investigation has shown that there are possible traces of malicious activities in Citrix Netscaler memory dumps, which are not detected by the above mentioned methods. This requires manual forensic investigation to be performed on the files.
The NCSC is able to investigate these files for known indicators for this
e

buiten verzoek

If you find any of these IOC's further investigation is needed to conclusively determine if the system is compromised. Please reach out to cert@ncsc.nl for further assistance.
[TLP:AMBER+STRICT]
-----BEGIN PGP SIGNATURE-----

5.1.1e

-----END PGP SIGNATURE-----