To: 5.1.2e @jio.nl]; 5.1.2e @jio.nl]
From: 5, 5.1.2e
Sent: Tue 8/26/2025 6:45:17 AM
Subject: RE: [TLP:GREEN] Update 6: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway - nieuwe checkscripts beschikbaar
Received: Tue 8/26/2025 6:45:17 AM

Beste Collega,
Het is zeker niet de bedoeling om een negatieve sfeer te creeren.
Ik denk dat een ieder weet hoe hard gewerkt is om de veiligheid te blijven garanderen. Laten we met elkaar het gesprek voeren hoe we dit soort situaties het hoofd bieden en zoregn dat we begrip hebben voor vragen als deze.
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 5.1.2e
M
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: zaterdag 23 augustus 2025 13:55
Aan: 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e < 5.1.2e @dji.minjus.nl>
Onderwerp: Re: [TLP:GREEN] Update 6: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway - nieuwe checkscripts beschikbaar

Thanks 5.1.2e ik schakel aankomende week ff met 5.1.2e ook over de inzet, kennis, expertise en misplaatst commentaar uit de omgeving
Fijne vakantie

Van: " 5.1.2 5.1.2e " < 5.1.2e @dji.minjus.nl>
Datum: vrijdag 22 augustus 2025 om 22:06:21
Aan: " 5, 5.1.2e < 5.1.2e @dji.minjus.nl>, 5.1.2e 5.1.2e " < 5.1.2e @dji.minjus.nl>
Onderwerp: RE: [TLP:GREEN] Update 6: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway - nieuwe checkscripts beschikbaar

Goedenavond 5.1.2e en 5.1.2e ,

Ik heb aan de mannen gevraagd om de scripts te draaien en de uitvoer naar jullie toe op te leveren. Mocht dat de komende dagen niet gebeuren: @ 5.1.2e wil je dan even schakelen met 5.1.2e

Weet dat dit veel sloopt bij de mannen die knijterhard hun best hebben gedaan voor een robuuste en veilige omgeving. Voor zover ik heb gehoord in de wandelgangen is er nog geen verdachte situatie gevonden in de achterliggende systemen, die is ontstaan naar aanleiding van de zero day kwetsbaarheid in de Netscalers. Zoals je hebt kunnen zien in de tijdlijn, hebben wij al heel vroeg een melding gedaan bij Citrix over crashende systemen en hebben we hen hierop constant bevraagd wat de status is. Onder andere de snelheid van patchen (binnen 6 uur heb ik vanmiddag gehoord) heeft er onder andere toe bijgedragen dat de schade (ook weer uit de wandelgangen) beperkt is gebleven.

Toch hebben de mannen een idee dat ze zich constant moeten verweren tegen de boze buitenwereld. En hierbij wordt gestoeid met frustraties van andere afdelingen en gebrek aan kennis van de omgeving. Daar worden zelfs de meest coole kikkers erg verdrietig van. Wellicht moeten we wat meer vertrouwen op onze specialisten en hen helpen de kwaliteit van hun werk onder de aandacht te brengen van anderen die wat minder inzicht hebben in de complexe infrastructuur van JIO voor haar opdrachtgevers,

Met vriendelijke groet,

5.1.2e 5.1.2e 5.1.2e
5.1.2e

Aanw: Di, Wo, Do, Vr

.....

Afdeling IPW
Justitiële ICT Organisatie
Ministerie van Veiligheid en Justitie
Stavorenweg 3 | 2803 PT | Gouda
Postbus 850 | 2800 AW | Gouda
.....
F
M 5.1.2e
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.
IT Denk aan het milieu: is uitprinten wel nodig?

-----Oorspronkelijk bericht-----
Van: 5.1 5.1.2e < 5.1.2e @dji.minjus.nl>
Verzonden: donderdag 21 augustus 2025 07:48
Aan: 5.1.2e @dji.minjus.nl>
CC: 5.1.2 5.1.2e >; 5.1.2e 5.1.2e @dji.minjus.nl>
Onderwerp: RE: [TLP:GREEN] Update 6: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway - nieuwe checkscripts beschikbaar

Beste 5.1.2e ,

Dank voor je reactie. Mijn advies is om deze Update 6 nog wel te laten uitvoeren op de Netscalers. Zeker omdat het nog niet volledig onder controle is en de schijnwerpers op dit onderwerp nog branden.
Dit zijn ook vragen die leven op management niveau bij JenV

Ik heb 5.1.2e in de CC meegenomen omdat hij hier ook vragen over krijgt vanuit de opdrachtgevers.

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 .1.2e
F 5.1.2e
M
Email: 5.1.2e @jio.nl

https://www.justitieleictorganisatie.nl

Volg ons ook op:

-----Oorspronkelijk bericht-----
Van: 5.1.2e , 5.1.2e < 5.1.2e @dji.minjus.nl>
Verzonden: woensdag 20 augustus 2025 16:41
Aan: 5.1 5.1.2e < 5.1.2e @dji.minjus.nl>
CC: 5.1.2e 5.1.2e < 5.1.2e >
Onderwerp: RE: [TLP:GREEN] Update 6: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway - nieuwe checkscripts beschikbaar

Goedemiddag 5.1.2e,

Wij hebben ons in deze laten leiden door de informatie en scripts die we vanuit Citrix hebben gekregen. De inhoud van deze scripts kwam overeen met het script van de NCSC.

We hebben alleen tijdens de grootste piek van de crisis de scripts gedraaid. Ik denk dat hiervan ook melding is gemaakt bij 5.1.2f. @5.1.2e kun je dit bevestigen of moet ik hier nog achteraan?

Met vriendelijke groet,

5.1.2e
Aanw: Di, Wo, Do, Vr
.....
Afdeling IPW
Justitiële ICT Organisatie
Ministerie van Veiligheid en Justitie
Stavorenweg 3 | 2803 PT | Gouda
Postbus 850 | 2800 AW | Gouda
.....
F
M 5.1.2e
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.
ΠDenk aan het milieu: is uitprinten wel nodig?

-----Oorspronkelijk bericht-----
Van: 5.1.2e < 5.1.2e @dji.minjus.nl>
Verzonden: woensdag 20 augustus 2025 15:37
Aan: 5.1.2e < 5.1.2e @dji.minjus.nl>
CC: 5.1.2e 5.1.2e < 5.1.2e >
Onderwerp: RE: [TLP:GREEN] Update 6: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway - nieuwe checkscripts beschikbaar

Beste 5.1.2e,

Dank voor je reactie. Specifiek was de vraag of de laatste update vanuit NCSC ook doorgevoerd is op de netscalers. Dat zie ik niet in de timeline

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 2e
F 5.1.2e
M
Email: 5.1.2e @jio.nl

https://www.justitieleictorganisatie.nl

Volg ons ook op:

-----Oorspronkelijk bericht-----
Van: 5.1.2 5.1.2e < 5.1.2e @dji.minjus.nl>
Verzonden: woensdag 20 augustus 2025 15:11
Aan: 5.1 5.1.2e < 5.1.2e @dji.minjus.nl>
CC: 5.1.2e i.1.2e < 5.1.2e >
Onderwerp: RE: [TLP:GREEN] Update 6: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway - nieuwe checkscripts beschikbaar

Goedemiddag 5.1.2e,

Zie de tijdlijn in de bijlage. Deze is ook al eerder gedeeld met 5.1.2f,2f .

Met vriendelijke groet,

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?

-----Oorspronkelijk bericht-----
Van: 5.1 5.1.2e < 5.1.2e @dji.minjus.nl>
Verzonden: woensdag 20 augustus 2025 14:30
Aan: 5.1.2 5.1.2e < 5.1.2e @dji.minjus.nl>
CC: 5.1.2e i.1.2e < 5.1.2e >
Onderwerp: FW: [TLP:GREEN] Update 6: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway - nieuwe checkscripts beschikbaar

Beste 5.1.2e,

Zie onderstaand.

Wil je aan de hand van een "timeline" aangeven welke maatregelen / controles uitgevoerd zijn zoals aangegeven in bijgaand schrijven op de netscalers

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 | Kamer 5.06 Laagbouw Postbus 850 | 2800 AW | Gouda .....
T 5.1.2e
F 5.1.2e
M
Email: 5.1.2e @jio.nl

https://www.justitieleictorganisatie.nl

Volg ons ook op:

-----Oorspronkelijk bericht-----
Van: 5.1.2i @lists.ncsc.nl>
Verzonden: woensdag 13 augustus 2025 12:37
Aan: 5.1.2i @ncsc.nl>
Onderwerp: [Rijksoverheid] Update 6: Aanvullende informatie over kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway - nieuwe checkscripts beschikbaar

-----BEGIN PGP SIGNED MESSAGE-----
5.1.2i

TLP:GREEN (https://first.org/tlp/)

Beste NCSC-partner,

Dit doelgroepbericht is een update van de doelgroepberichten over twee actief misbruikte kwetsbaarheden in Citrix Netscaler ADC en Netscaler Gateway die op vrijdag 4, vrijdag 18, maandag 21, dinsdag 22, vrijdag 25 en maandag 28 juli zijn verstuurd. Op maandag 11 augustus heeft het NCSC een nieuw websitebericht met duiding van deze casus met handelingsperspectief geplaatst op www.ncsc.nl/citrix.
Hieronder lees je hoe je zelf onderzoek kan doen kan doen met behulp van de twee volledig nieuwe checkscripts die het NCSC heeft ontwikkeld. Als forensisch onderzoek door middel van de checkscripts niet (tijdig) wordt uitgevoerd, is de kans groot dat compromittatie van systemen onopgemerkt zal blijven en de kwaadwillende actor toegang behoudt.
Deze checkscripts zijn terug te vinden op de Github-pagina van het NCSC:
https://github.com/NCSC-NL/citrix-2025 . Het script is TLP:CLEAR.
Het ene checkscript richt zich op coredumps, het andere checkscript richt zich op complete NetScaler images. Onder het kopje handelingsperspectief wordt kort het verschil tussen de twee verschillende checkscripts uitgelegd. Hoe je de scripts moet uitvoeren is terug te lezen in de readme-files die op de Github staan.
De checkscripts zijn voorzien van nieuwe indicators of compromise die zijn geïdentificeerd naar aanleiding van recent forensisch onderzoek van het NCSC en zijn nog niet eerder gecommuniceerd. Hierdoor worden organisaties opgeroepen om de nieuwe checkscripts uit te voeren op hun Citrix NetScaler apparaten.
Informatiedeling: Door het actief delen van informatie kan het NCSC het onderzoek beter uitvoeren, omdat de bevindingen elkaar versterken Samen krijgen we steeds meer zicht op de impact die deze aanvallen hebben zodat we daar passend op kunnen reageren.

=== Feiten ===
* Op basis van nieuwe inzichten heeft het NCSC twee nieuwe checkscripts ontwikkeld. De nieuwe checkscripts zijn te vinden op https://github.com/NCSC-NL/citrix-2025.
* Het NCSC stelt vast dat er meerdere kritieke organisaties binnen Nederland succesvol aangevallen zijn.
* Zero-day kwetsbaarheid: Nader onderzoek wijst uit dat de kwetsbaarheid ten minste vanaf begin mei is misbruikt door de actor. Op 25 juni publiceerde Citrix informatie over kwetsbaarheid CVE-2025-6543 en bood een patch aan om deze te verhelpen. We spreken hiertoe over een zero-day aanval, aangezien de kwetsbaarheid is misbruikt voordat deze publiek bekend werd gemaakt.
* Actief sporen gewist: Forensisch onderzoek bij getroffen organisaties laat zien dat er actief sporen zijn uitgewist door de aanvaller.
* Indicator of Compromise: De casus is in ontwikkeling; indien er additionele deelbare IoC's of handelingsperspectieven beschikbaar komen, zal het NCSC hierover communiceren.

=== Duiding ===
* Geavanceerde actor: Het feit dat er sprake is van een zero-day kwetsbaarheid en dat de actor(en) onder de radar proberen te blijven weergeeft de geavanceerde capaciteiten van deze actor(en).
* Voortdurend onderzoek: Doordat het onderzoek door het NCSC en de organisaties nog loopt is er geen totaal aantal getroffen organisaties vast te stellen.

=== Handelingsperspectief ===
Checkscripts:
* Voer zelf onderzoek uit naar sporen van compromittatie:
* Voer scans met de nieuwste checkscripts uit (zie Github), om de NetScaler
ADC- en NetScaler Gateway-systemen te controleren op mogelijke compromittatie.
* Beide scripts zijn bedoeld om onderzoek uit te voeren op reeds veiliggestelde NetScaler systemen en/of data.

1. Forensisch image scan script
a. Dit script kan forensische kopieën, en VM's, van Netscaler systemen openen en hun inhoud controleren op de aanwezigheid van malafide indicatoren.
b. Het script gebruikt Dissect van 5.1.2f , waardoor het niet uitmaakt naar welk formaat het NetScaler systeem is veiliggesteld (dd, xvz of e01).
c. Het script checkt op reeds bekende malafide indicatoren die gerelateerd zijn aan de recente NetScaler aanvallen, maar het voert ook een

controle uit op andere malafide indicatoren.
d. De resultaten van het script worden weggeschreven naar een bestand dat gedeeld kan worden met het NCSC. Graag ontvangen wij ook desbetreffende kopie/VM ook via 5.1.2e@ncsc.nl.
e. Instructies voor het installeren en configureren van het script zijn bijgevoegd en terug te vinden op de Github.

2. Coredump scan script
a. Dit script kan de inhoud van coredump bestanden controleren op de aanwezigheid van malafide indicatoren. Coredump bestanden worden aangemaakt wanneer een proces crasht, mogelijkerwijs door pogingen van exploitatie.
Een coredump bevat het geheugen van het proces dat crasht, waardoor mogelijke sporen van actor(en) aanwezig zijn.
b. Met dit script kunnen de coredumps, welke geëxtraheerd zijn uit de NetScaler systemen, gecontroleerd worden op malafide indicatoren. De resultaten worden weggeschreven naar een bestand welke gedeeld kan worden met het NCSC. Graag ontvangen wij ook desbetreffende coredumps ook via 5.1.2e@ncsc.nl.
c. Instructies voor het installeren en configureren van het script zijn bijgevoegd en terug te vinden op de Github.

Algemeen handelingsperspectief:
* Verhoog digitale weerbaarheid: Richt governance [1] goed in, en tref basismaatregelen [2].
* Weet wat je beschermt: Breng organisatiebelangen [3] in beeld en richt kwetsbaarhedenbeheer [4] in.
* Zorg voor een gelaagde verdediging: Het NCSC onderstreept daarom dat een defense-in-depth strategie toegepast moet worden, waarbij er meerdere lagen van verdediging opgezet worden om de weerbaarheid zo te verhogen. Als een aanvaller dan één maatregel weet te passeren, dan zijn jouw te beschermen belangen niet direct gecompromitteerd.
* Wees voorbereid: Zorg dat je als organisatie klaar bent om te detecteren [5], reageren [6], onderzoeken [7] en herstellen [8] als je getroffen word.

* Blijf het NCSC volgen: Op deze pagina [9] kan je meer informatie vinden over bijstand van het NCSC en het maken van een melding. Op www.ncsc.nl/citrix kan je meer informatie vinden over de kwetsbaarheden in Citrix NetScaler ADC en NetScaler Gateway. En voor contact met het NCSC kunt u terecht op www.ncsc.nl/contact of via 5.1.2e@ncsc.nl voor directe meldingen.
* Raadpleeg de NCSC website en de doelgroepberichten die op vrijdag 18 juli, maandag 21 juli, dinsdag 22 en maandag 28 juli jl. zijn verstuurd, zodat je de eerder gedeelde informatie en het handelingsperspectief kunt nalezen.
* Indien je verdenkt dat jouw Citrix Netscaler ADC en Netscaler Gateway systemen gecompromitteerd zijn door het aantreffen van een of meer van de bovengenoemde IOC's, neem contact op met 5.1.2e@ncsc.nl

** ENGLISH VERSION **

Dear NCSC-partner,

This message is an update to the messages about two actively exploited vulnerabilities in Citrix Netscaler ADC and Netscaler Gateway. On August 11, 2025 the NCSC published a new post on it's website with the analysis en course of action which you can find on www.ncsc.nl/citrix.
Any new information that the NCSC receives will be shared with as many organizations as possible to enable them to do technical analysis of their Citrix systems. The NCSC strongly emphasizes to take the advised courses of action as detailed below.
This message details how you can do research and forensic analysis yourself using two completely new versions of the checkscripts created by the NCSC.
The first checkscript focusses on coredumps, the other on complete forensic NetScaler images. In the Course of Action paragraph the difference between the two scripts is briefly explained. How to use the scripts for you own analysis is described in readme-files published on https://github.com/NCSC-NL/citrix-2025 . The script is TLP:CLEAR.
Within the checkscripts are new indicators of compromise that have been identified after recent forensic research by the NCSC which not have been communicated before. Organizations are advised to run the new checkscripts on their Citrix NetScaler appliances.
If technical analysis with the new checkscripts is postponed or skipped, it increases the chance that any compromise will go unnoticed and and that the actor will maintain persistent access to your organization.
Information sharing: As organizations continue to actively share information, the NCSC is able to improve ongoing analysis and enrich its results. Together we are getting a better scope on the impact of these attacks so that we are able to respond accordingly.

=== Facts ===
* Based on new insights the NCSC created two completely new checkscripts.
These new checkscripts are published on
https://github.com/NCSC-NL/citrix-2025 .
* The NCSC confirms that multiple critical organizations within the Netherlands have been succesfully compromised.
* Zero-day vulnerability: Further research shows that the vulnerability has been exploited by attackers sinde early May 2025. On June 25th, 2025 Citrix published an advisory on vulnerability CVE-2025-6543 with a patch to remediate the vulnerability. Therefore, the vulnerability is marked as zero-day as active exploitation happened before public knowledge of the vulnerability.
* Removal of evidence: Forensic research at compromised organizations shows that the acttack has actively removed traces on targeted systems.
* Indicator of Compromise: This case is in ongoing development. When additional IoCs or courses of action become available, the NCSC will communicate about this.

=== Interpretation ===
* Advanced actor: Based on the fact that the actor(s) used a zero-day vulnerability and actively operates under the radar can be assessed as having advanced capabilities.
* Ongoing investigation: Due to the fact that the investigations of both the organizations and the NCSC are still ongoing, no final number of

compromised organization can be determined.

=== Course of action ===
Checkscripts:
* Investigate your systems for traces of compromittation
* Use the newest checkscripts (see Github) to determine whether your NetScaler ADC and NetScaler Gateway-systems could have been compromised .
* Both scripts are designed to be applied on already secured data from the NetScaler systems.

1. Forensic image scan script
a. This script can open forensic copies, and VM's of Netscaler systems and check their content on the presence of indicators of compromise.
b. The script uses Dissect made by 5.1.2f, because of which it does not matter what format from the NetScaler system has been secured (dd, xvz or e01).
c. The script checks on known indicators of compromise, related to the recent NetScaler attacks but also checks on other indicators of malicious activity.
d. The results of the scrips are dumped to a file that can be shared with the NCSC. We would like to receive these results via 5.1.2e@ncsc.nl.
e. Instructions for installation and configuration for the script are also enclosed.

2. Coredump scan script
a. This script can check the contents of the coredump files for the presence of indicators of compromise. Cordump files are created when a process fails. Failure, and the creation of a coredump file can indicated an exploitation attempt. A coredump contains the memory of the process that crashes, this can contain traces of malicious activity.
b. The results of this script are dumped to a file that can be shared with the NCSC. We would kindly request that you share these results including the coredump itself with us via 5.1.2e@ncsc.nl.
c. Instructions for installation and configuration of the script are also enclosed.

General courses of action:

* Improve digital resilience: Organise good governance [1], take basis securitymeasures [2].
* Know what you need to protect: Identify organisation goals [3] and provide sufficient vulnerabiltiymanagement [4].
* Provide layered security: The NCSC highlight that a defense-in-depth strategy should be applied. Multiple layers of security should be created to improve digital resilience. This makes sure that the malicious attacker that manages to bypass 1 securitymeasure does not have direct access to your vital assets.
* Be prepared: Provide the plans an means to detect [5], respond [6], investigate [7] and recover [8] when incidents happen.
* Follow NCSC updates: On this page [9] more information on NCSC support and the alerting can be found. On this page[10] more information on the vulnerabilties in Citrix NetScaler ADC and NetScaler Gateway is published.
For contact with the NCSC please visit this page[11] or make a direct alert through 5.1.2e@ncsc.nl.
* Check the NCSC website NCSC-partner updates of Friday July 18, Monday July 21, Tuesday 22 and Monday July 28. These provide more information on the vulnerabilities and courses of action.
* When you suspect your Citrix Netscaler ADC and/or Netscaler Gateway systems of being compromised because of the presence of one or more IOCs, please contact 5.1.2e@ncsc.nl

If you have any questions and/or remarks regarding this product, please contact NCSC-NL through your point of contact or 5.1.2e@ncsc.nl. If you want to contact NCSC-NL regarding suspicious behavior of possible compromise of a Citrix system, contact 5.1.2e@ncsc.nl. NCSC-NL gladly receives technical indicators.

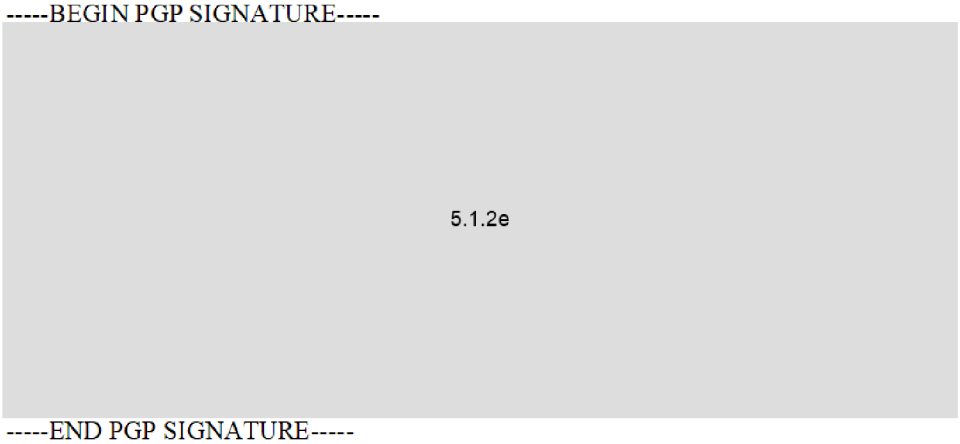
[1]https://www.ncsc.nl/wat-kun-je-zelf-doen/routekaart-risicomanagement
/governance-en-randvoorwaardenity Centrum [2]https://www.ncsc.nl/wat-kun-je-zelf-doen/basisprincipes
[3]https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herkennen/hoe-
breng-ik-mijn-te-beschermen-belangen-in-kaart
[4]https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/detecteren
/kwetsbaarhedenbeheer
[5]https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/detecteren
/detectie-in-cybersecurity
[6]https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/reageren/incident-
respons-waar-begin-ik
[7]https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/beschermen
/forensic
[8]https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herstellen
/herstel-van-een-cyberincident
[9] https://www.ncsc.nl/wat-doet-het-ncsc-voor-jou/incident-respons
[10] https://www.ncsc.nl/citrix
[11]https://www.ncsc.nl/contact

[\TLP:GREEN]

Met vriendelijke groet,

Nationaal Cyber Security Centrum
Postbus 117 | 2501 CC | Den Haag | www.ncsc.nl
E 5.1.2e@ncsc.nl
T +31 70 751 55 55 (algemeen)
PGP 5.1.2e
Bezoekadres:
Turfmarkt 147 | 2511 DP | Den Haag

-----BEGIN PGP SIGNATURE-----



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

Rijksoverheid maillijst -- 5.1.2i @lists.ncsc.nl Stuur een e-mail naar 5.1.2i @lists.ncsc.nl om je uit te schrijven