5.1.2e 5.1.2e

Van: 5.1.2e 5.1.2e
Verzonden: dinsdag 29 juli 2025 15:59
Aan: 5.1.2e 5.1.2e
CC: 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e
Onderwerp: RE: Overzicht openstaande acties DJI aan JIO irt crisissituatie - URGENT

5.1.2e

Hieronder even in het kort een aanvullende reactie (in het rood) op de vragen die door jou zijn gesteld.

Met vriendelijke groet,

5.1.2e

Van: 5.1.2e 5.1.2e
Verzonden: donderdag 24 juli 2025 11:27
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 @dji.minjus.nl>
Onderwerp: RE: Overzicht openstaande acties DJI aan JIO irt crisissituatie - URGENT

5.1.2e hieronder in het blauw onze reactie op de rood gemarkeerde punten.

Van: 5.1.2e 5.1.2e) < 5.1.2e @dji.minjus.nl>
Verzonden: donderdag 24 juli 2025 09:14
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 @dji.minjus.nl>
Onderwerp: FW: Overzicht openstaande acties DJI aan JIO irt crisissituatie - URGENT
Urgentie: Hoog

Hi 5.1.2e
In opvolging van de mail van 5.1.2e moet DI om 11:00 een actieplan voorleggen aan het DJI-CCD.
Kun jij voor 11:00 een eerste beantwoording geven, met prioriteit op de rood gemarkeerde zaken?
Bv. Wat zijn de stappen/acties om wachtwoord reset te activeren?

Ik bel je zo even.

Grtz. 5.1.2e

Met vriendelijke groet,

5.1.2e 5.1.2e 5.1.2e
.....
Directie Informatievoorziening – Functioneel Beheer & Dienstenmanagement
Dienst Justitiële Inrichtingen
Ministerie van Justitie en Veiligheid
Bezoekadres: Turfmarkt 147 | 2511 DP | Den Haag
Postadres: Postbus 30132 | 2500 GC | Den Haag
.....
T 5.1.2e
5.1.2e @dji.minjus.nl
http://di-dji-intranet.minvenj.nl/

.....

Aanwezig op: ma. di. wo. en do.
.....

Van: 5.1.2e 5.1.2e <5.1.2e @dji.minjus.nl>
Verzonden: woensdag 23 juli 2025 20:05
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 @dji.minjus.nl>; 5.1.2e 1.2e 5.1.2e @dji.minjus.nl>; 5.1.2e 5.1.2e <5.1.2e n@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 e <j.d.visser@dji.minjus.nl>
Onderwerp: Overzicht openstaande acties DJI aan JIO irt crisissituatie
Urgentie: Hoog

Beste 5.1.2e

Vandaag - 23 juli - is er weer op verschillende vlakken afstemming geweest tussen DJI en JIO over het lopende incident m.b.t. de inbreuk op een van de Netscalers, het onderzoek daarop en scenarios gericht op mitigatie en anticipatie op 'wat als' er in het onderzoek iets wordt gevonden dat voor ons allen slecht nieuws is. Dit bericht is bedoeld als samenvatting van de verschillende punten die daarbij tussen DJI en JIO zijn besproken en afgesproken. Daarbij is dit ook een formele bevestiging daarvan, vanuit mijn rol binnen DJI.

CISO afstemmingsoverleg (Voorgezeten door 5.1.2e 5. 5.1.2e

- DJI verwacht van JIO een advies op handelingsperspectief en risicoduiding. Specifiek daarin zijn we op zoek naar de vraag of we verantwoord online kunnen blijven, zonder dat nu ernstig risico kan worden uitgesloten in afwachting op het onderzoeksresultaat.
  Het advies vanuit JIO is de afgelopen dagen onverminderd hetzelfde: Wij adviseren om nu de systemen niet geheel af te sluiten van het internet en offline te gaan, omdat er geen bewijzen zijn dat er verder is doorgedrongen tot de beveiligde zone. Zoals onlangs in de communicatie ook aan de CIO's is aangegeven: JIO geeft hierover een advies en de opdrachtgever neemt (in overleg met de eigenaar en de 5.1.2e zelf het besluit hierover.

- JIO kan op dit moment niet uitsluiten dat de aanvaller vanuit de verworven positie op de Netscaler in staat is geweest om logingegevens van DJI of andere gebruikende organisaties te bemachtigen. DJI houdt er daarom sterk rekening mee dat dit mogelijk heeft plaatsgevonden en wil hierop mitigerende maatregelen treffen. DJI verwacht van JIO voorbereiding op het doorvoeren van een geforceerde wachtwoord reset voor alle accounts die hierin mogelijk getroffen zijn. Zie bijgevoegde memo hierover. Dit heeft grote urgentie want vrijdag staat besluitvorming hieromtrent binnen DJI gepland.
  Geforceerde wachtwoord reset voor DJI is inmiddels uitgevoerd. Voor DT&V en JIO zal dit komende dagen worden opgepakt.

- DJI verwacht een schriftelijke rapportage op de voortgang en bevindingen van het Compromised Assessment tot zover. We wensen daarna dagelijks updates hierop te ontvangen en ook zodra zich op dit vlak belangrijke ontwikkelingen (positief danwel negatief) voordoen. 5.1.2e heeft aan JIO benadrukt dat volledige transparantie daarbij voor ons noodzakelijk is, mede gezien de bestuurlijke druk.
  We rapporteren dagelijks de status vanuit het technisch onderzoek zowel richting de CISO's in de dagelijkse sessies om 13.00 als richting het hogere management middels een Sitrap

- DJI verwacht een schriftelijke rapportage van voorgenomen en reeds uitgevoerde mitigerende maatregelen tot dusver. Wij hebben hierover wel geregeld updates ontvangen, maar we hebben sterk behoefte aan een integraal beeld. Als onderdeel daarvan op welke wijze het gecompromitteerde Netscaler systeem geïsoleerd is? Is dit in het netwerk afgesloten, helemaal offline gezet, opnieuw geinstalleerd, etc?

Het volgende is uitgevoerd aan mitigerende maatregelen:

Op de dag van publicatie van beide kwetsbaarheden (CVE2025-5777 17 juni, CVE2025-6543 25 juni) zijn de updates geinstalleerd op Netscalers en zijn de mitigerende maatregelen zoals voorgeschreven door Citrix uitgevoerd op de aan het internet gekoppelde Netscalers. Voor beide kwetsbaarheden zijn op de opvolgende werkdagen (18 en 26 juni) dezelfde werkzaamheden uitgevoerd op de interne Netscalers.

Op 8 juli is JIO op de hoogte gebracht door Citrix over de bevinding dat er een achterdeur is gevonden op één specifieke Netscaler. Er is toen nog geen incident response opgestart om uit te sluiten dat de aanvaller verder is doorgestapt in het netwerk. Wel zijn er aditionele mitigerende maatregelen genomen zoals het resetten van service accounts die actief zijn op de Netscalers en certificaten die door de Netscalers worden gebruikt t.b.v. authenticatie. De aangetroffen achterdeur is verwijderd en op basis van het huidige beeld van 5.1.2f zijn de Netscalers niet langer gecompromiteerd sinds 8 juli 2025.

Momenteel is 5.1.2f bezig onderzoek te verrichten op drie verschillende trajecten, onderzoek op Netscaler, onderzoek op omliggende netwerk en onderzoek op interne DWO omgeving en worden hierin ondersteund door het pentest team en het SOC JIO en het SOC JenV. Daarnaast zijn er gaten geidentificeerd in de dekkingsgraad van de monitoring, hier wordt door JIO i.s.m. 5.1.2f aan gewerkt.

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

1. Opname Netscalers in SIEM; Technisch vandaag (24-7) gereed;
2. Uitbreiden toezicht/monitoring op de Domain Controllers; Technische test vinden nu plaats;
3. Installeren 5.1.2h agents op de DWO; Technische tests vinden nu plaats in de test omgeving.

Het advies vanuit JIO is de afgelopen dagen onverminderd hetzelfde: Wij adviseren om nu de systemen niet geheel af te sluiten van het internet en offline te gaan, omdat er geen bewijzen zijn dat er verder is doorgedrongen tot de beveiligde zone.
Zoals gisteren in de communicatie ook aan de CIO's is aangegeven: JIO geeft hierover een advies en de opdrachtgever neemt (in overleg met de eigenaar en de 5.1.2e zelf het besluit hierover. Wij hebben met het NCSC gesproken over mogelijke stappen en hebben hun advies opgevolgd om een compromised assessment uit te voeren. Wij voeren op dit moment met externe leveranciers dit onderzoek uit. Ook het Team High Tech Crime van de politie is aangesloten en was gisteren en vandaag aanwezig in Gouda.

Ons advies is gebaseerd op het feit dat één Netscaler is gecompromitteerd, maar er vooralsnog geen bewijzen zijn dat ze ook doorgedrongen zijn tot de beveiligde zone. Daarnaast zetten wij in op verhoogde monitoring en detectie.

Verkenning handelingsperspectief en wat-als scenario's (Voorgezeten door 5.1.2e 5.1.2e

- Wij hebben in deze overlegsetting vanuit DJI toegelicht dat we als mitigerende maatregel inzetten op een wachtwoordwijziging. Dit voor het geval dat de aanvaller in de positie op de Netscaler in staat is geweest om lgingegevens te bemacvchtigen. Zie voorgaand en memo.

Deze preventieve maatregel gaan wij in gang zetten. 5.1.2e zal hierover contact opnemen met DT&V om deze preventieve maatregel ook bij DT&V in te zetten. (Uiteraard zullen we deze maatregel ook voor de JIO populatie in gang gaan zetten.
Deze actie is inmiddels uitgevoerd voor DJI

- Lopende het onderzoek houdt DJI er rekening mee dat de impact groter is dan tot nu toe blijkt. Zolang dit niet kan worden uitgesloten bereidt DJI zich daarop voor. We voorzien daarbij twee isolatie-scenario's die mogelijk na of naast elkaar zouden kunnen optreden. JIO heeft ons geinformeerd dat verkend wordt of dergelijke isolatie in zowel scenario 1 als scenario twee mogelijk ook gedeeltelijk mogelijk is, zodat essentiele verkeersstromen kunnen blijven plaatsvinden, terwijl risico in deze eventuele situaties wel in belangrijke mate wordt teruggebracht.
    1. Internet, van buiten naar binnen en van binnen naar buiten: Als onderzoek uitwijst dat een aanvaller dieper in de infrastructuur is binnengedrongen dan is er risico dat die aanvaller nog binnen is en ook in staat is met onze omgeving te blijven communiceren om een aanval voort te zetten. In dat geval is een mogelijke mitigerende maatregel om onze verbindingen met internet geheel of gedeeltelijk te isoleren, om daarmee zeker te stellen dat we de aanvaller daarmee de pas afsnijden.

       Van buiten naar binnen: Als de internetverbinding van buiten naar binnen wordt afgebroken, dan is Connect niet meer toegankelijk. JIO onderzoekt om dit selectief bereikbaar te houden op basis van het netwerk vanwaar een gebruiker afkomstig is. Met Solvinity wordt gekeken of bijv verkeer vanaf Govroam en de Wifi van de Turfmarkt selectief kan worden toegelaten.

DJI vormt beeld of er in onze ketensamenwerking externe organisaties zijn (bijv zorgpartners) die gebruik maken van Connect om zo bij DJI informatiesystemen te komen.

Van binnen naar buiten: JIO heeft toegelicht dat internetverkeer van binnen naar buiten voor zowel gebruikers als voor applicaties verloopt via dezelfde paden (proxy infrastructuur). Voor applicaties is dat op basis van IP adressen.
DJI verzoekt JIO om een lijst van deze IP-adressen en bijbehorende functionele namen (FQDN's), zodat wij dit kunnen gebruiken bij impactbepaling en uitwerking voor dit scenario.
JIO heeft ons toegelicht dat sommige applicaties 5.1.2h andere paden hebben 5.1.2h DJI verzoekt JIO om een overzicht daarvan aan te leveren, zodat wij dit kunnen gebruiken bij impactbepaling en uitwerking voor dit scenario.

Er zijn inmiddels meerdere sessies geweest met DJI om dit verder uit te werken. Het concept handelingskader wordt dagelijks in samenspraak verder uitgebouwd.

2. Quarantaine: Als onderzoek uitwijst dat de DWO gecompromitteerd is, dan is niet uit te sluiten dat een aanvaller nog aanwezig is en via JustitieNet mogelijk ook naar andere organisaties (in 5.1.2h termen: 5.1.2h) kan proberen door te dringen. Om te zorgen dat een compromitatie niet als een cascade van de ene naar de andere omgeving kan uitbreiden is er in 5.1.2h daarvoor een quarantaine dienst.
JIO heeft aan ons toegelicht dat het mogelijk is om in de quarantainedienst specifieke verkeersstromen uit te zonderen (die kunnen dan dus wel doorlopen).
DJI verzoekt om op dit scenario te anticiperen en een impactbepaling op te stellen voor het geval quarantaine moet worden ingesteld. DJI vraagt hierin om advies op welke wijze dit selectief kan, zodat risico zoveel mogelijk gereduceerd wordt en essentieel verkeer toch zoveel als mogelijk kan blijven plaatsvinden.

Zie punt 1

DJI vraagt aan JIO om op de verschillende verzoeken via de lopende crisislijnen en -overleggen terug te koppelen en daar ook een tijdslijn bij aan te geven. Dit is veel, dat besef ik terdege. DJI ziet hierin absoluut het harde werk en de inzet van JIO, dit is een manier om de energie te richten op besluitvorming waar iedereen baat bij heeft.

Met vriendelijke groet,

5.1.2e

5.1.2e

Dienst Justitiële Inrichtingen
Ministerie van Justitie en Veiligheid
5.1.2e
5.1.2e @dji.minjus.nl