Justitiële ICT Organisatie
Ministerie van Justitie en Veiligheid

Ministerie van Justitie en Veiligheid
Directie Informatievoorziening en Inkoop (DI&I)

Justitiële ICT Organisatie
Implementatie en
Dienstverlening,
Programma's, Projecten,
Architectuur en Security

Stavorenweg 3
2803 PT Gouda
Postbus 850
2800 AW Gouda
www.justitieleictorganisatie.nl

5.1.2e 5.1.2e
5.1.2e
5.1.2e
5.1.2e

nota

Bevindingen 5.1.2h juli 2025
TLP:AMBER

Datum
1 augustus 2025

Ons kenmerk
5.1.2h Juli 2025

Van
5.1.2e 5.1.2e
Datum/eindparaaf

5.1.2e 5.1.2e
Datum/paraaf

5.1.2e 5.1.2e
Datum/paraaf

5.1.2e
Datum/paraaf

Kopie aan
Solvinity
Datum/paraaf

Concipiënt
Datum/paraaf

Inleiding

Halverwege juni 2025 is er een zero day kwetsbaarheid geconstateerd in het Citrix NetScaler platform. Het Citrix NetScaler platform wordt binnen het Rijk door o.a. Justitiële ICT Organisatie (JIO) ingezet als Gateway voor het beschikbaar stellen van de virtuele KA Desktops (werkplekken).

5.1.2h

Deze NetScalers worden gehost in 5.1.2h het koppelvlak tussen Internet en 5.1.2h 5.1.2h wordt door Solvinity beheerd in opdracht van Directie Informatievoorziening en Inkoop (DI&I).

5.1.1c

Justitiële ICT Organisatie
Implementatie en Dienstverlening, Programma's, Projecten, Architectuur en Security

Datum
1 augustus 2025

Ons kenmerk
5.1.2h Juli 2025

JIO heeft geconstateerd dat de zero day kwetsbaarheid op de NetScalers van DJI actief is misbruikt, waarna een onderzoek en impactanalyse is gestart.

Tijdens dat onderzoek is geconstateerd dat het verkeer in 5.1.2h meer openstaat, dan conform het ontwerp van 5.1.2h toegestaan is en dat dit een aanzienlijk risico is voor de diensten van de deelnemers in 5.1.2h

In deze nota wordt deze toegelicht en advies gegeven over de verdere handelingen.

Toelichting

Woensdag 30 juli is er in samenwerking tussen 5.1.2h en JIO een configuratiefout geconstateerd in de 5.1.2h Zone firewall. Deze firewall beveiligt alle verkeersstromen tussen alle virtuele- en fysieke servers binnen 5.1.2h

Binnen 5.1.2h,5.1.2i (DMZ / Voorportaal van 5.1.2h) worden informatievoorzieningen van alle deelnemers van JenV gehost. Hieronder vallen o.a. ook de NetScaler diensten voor thuiswerken en ook business applicaties.

Onderdeel van de beveiliging in 5.1.2h is een categorisering van de netwerken in drie veiligheidszones en een compartimentering van diensten binnen die zones. Het doel van deze compartimentering is het verkleinen van het foutdomein, waardoor het compromitteren van één dienst niet (eenvoudig) andere systemen in gevaar brengt.

5.1.2h,5.1.2i is op opgedeeld in drie veiligheidszones[1]:

- ***Trust Level 1 (TL1)**: (publiek)* 5.1.2h
  5.1.2h
- ***Access Level 1 (AL1)**: (beperkt)* 5.1.2h
  5.1.2h
- ***Trust Level 2 (TL2)**: (besloten)* 5.1.2h
  5.1.2h

Uit de test die door JIO op 27 juli 2025 is afgerond, 5.1.2h
5.1.2h
5.1.2h Deze resultaten zijn op 28 juli 2025 gemeld.

5.1.2h

5.1.1c

Justitiële ICT Organisatie
Implementatie en Dienstverlening, Programma's, Projecten, Architectuur en Security

Datum
1 augustus 2025

Ons kenmerk
5.1.2h Juli 2025

Tijdens het onderzoek dat door 5.1.2h en JIO is uitgevoerd op 30 juli 2025 is een configuratiefout in de zone firewall geconstateerd. 5.1.2h

5.1.2h

Risico's mitigerende maatregelen

5.1.2h

5.1.2h

5.1.2h

5.1.2h

5.1.2h

168346316 0013 0051

Justitiële ICT Organisatie
Implementatie en
Dienstverlening,
Programma's, Projecten,
Architectuur en Security

Datum
1 augustus 2025

Ons kenmerk
5.1.2h Juli 2025

Stand van zaken

De configuratiefout in de firewall is door 5.1.2h op 30 juli 2025 hersteld. Daarbij is ook onderzocht of er verdachte verkeersstromen zich op dat moment voordeden. Op basis van de mogelijkheden tot forensisch onderzoek zijn geen verdachte, maar wel functioneel niet gewenste stromen ontdekt.

Advies



Korte termijn

Op korte termijn is het advies om de volgende acties uit te voeren:

- Root cause analyze om de oorzaak en niet alleen het symptoom te bestrijden.
- Audit en test procedures en beleid nalopen om te zorgen dat deze scope voortaan ook regelmatig wordt onderzocht.
- Opnieuw uitvoeren van de netwerk scan door JIO. Reeds in gang gezet.
- Gevonden kwetsbaarheid direct melden bij alle deelnemers van 5.1.2h
- Uitvoeren van scans op verdachte accounts[2] van de Active Directories van **ALLE** deelnemers, niet alleen opdrachtgevers van JIO.
- Uitvoeren van het onderzoek naar compromittatie van potentieel kwetsbare systemen van alle deelnemers in de ODC's.
- Uitvoeren van een vulnerabillity scan over heel 5.1.2h en op basis van resultaten herstellen van de kwetsbaarheden.
- Doornemen van het verkeer en het afsluiten van alle niet gebruikte netwerkstromen.
- Verhoogd toezicht op het verkeer binnen het compartiment op mogelijk afwijkend en verdacht verkeer.
- Creëren en bijhouden van een gedetailleerde architectuurplaat[3] waarin alle relevantie informatie in opgenomen is die noodzakelijk is om inzicht te krijgen in de netwerkstromen.

[2] Dit is cruciaal omdat een aanvaller om persistente toegang te realiseren een "regulier" gebruikersaccount in AD aan zal maken om persistent toegang te hebben. Daarmee is er geen backdoor / kwetsbaarheid meer nodig.
[3] Eventueel zijn hier tools / platformen voor die dit inzicht geautomatiseerd creëren en bijhouden. Dit zou verder moeten worden onderzocht.

168346316 0013 0052

Justitiële ICT Organisatie
Implementatie en
Dienstverlening,
Programma's, Projecten,
Architectuur en Security

Datum
1 augustus 2025

Ons kenmerk
5.1.2h Juli 2025

Middellange termijn

Op lange termijn is het advies om de volgende acties uit te voeren:

- Het verbeteren van het wijzigings- en registratieproces om configuratiefouten te vóórkomen.

5.1.2h

5.1.2h

5.1.2h

Met vriendelijke groet,

Justitiële ICT Organisatie