To: 5.1.2e [5.1.2e @jio.nl]; 5.1.2e 5.1.2e [5.1.2e @jio.nl]
From: 5.1.2e , 5.1.2e
Sent: Tue 3/3/2026 4:44:14 PM
Subject: Fwd: Vragen Argos (VPRO) over hack JIO via Citrix kwetsbaarheid
Received: Tue 3/3/2026 4:44:15 PM

Hier alvast de vragen

Van: " 5.1.2e 5.1.2e < 5.1.2e @minjenv.nl>
Datum: dinsdag 3 maart 2026 om 17:31:53
Aan: " 5.1.2e , 5.1.2e " < 5.1.2e @jio.nl>
Onderwerp: FW: Vragen Argos (VPRO) over hack JIO via Citrix kwetsbaarheid

Hi 5.1.2e ,
We hebben vandaag een set persvragen ontvangen over het Citrix-incident bij JIO afgelopen zomer.
Na een snelle analyse lijkt het overgrote deel niet beantwoord te worden in de Kamerbrief; zie de rood/groene arceringen in de set.
Kunnen jullie de vragen die aan jullie gesteld worden beantwoorden? Dan zorgen wij voor de beantwoording aan onze kant.
5.1.2e 5.1.2e leest graag mee op het totaalpakket. Wij zullen ook zorgen dat de definitieve beantwoording (na goedkeuring/afstemming) vervolgens weer bij woordvoering terecht komt.
Ivm deadline van de journalist; kun je aangeven of het jullie lukt einde deze week (donderdag/vrijdag) de input aan te leveren? Als dat niet haalbaar is, ook prima, laat vooral weten dan kan woordvoering met de journalist schakelen!
Alvast dank en ik hoor graag!
Met vriendelijke groet,
5.1.2e

.....
Ministerie van Justitie en Veiligheid
Ministerie van Asiel en Migratie
Directie Informatievoorziening en Inkoop
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
M - 5.1.2e
E 5.1.2e @minjenv.nl
www.rijksoverheid.nl/jenv
www.rijksoverheid.nl/aenm
.....
Met recht voor iedereen
.....

Van: 5.1.2e . - 5.1.2e < 5.1.2e @minjenv.nl>
Verzonden: dinsdag 3 maart 2026 14:53
Aan: 5.1.2e 5.1.2e 5.1.2e @minjenv.nl>
CC: 5.1.2e , 5.1.2e < 5.1.2e @minjenv.nl>
Onderwerp: FW: Vragen Argos (VPRO) over hack JIO via Citrix kwetsbaarheid

Hi 5.1.2e
Onderstaand is een set vragen die wij van 5.1.2e 5.1.2e van Argos hebben ontvangen. Nu heb ik het vermoeden dat de journalist de kamerbrief niet heeft gelezen aangezien het in deze kamerbrief redelijk wordt beantwoord Kamerbrief over impact strafrechtketen informatiebeveiliging OM | Kamerstuk | Rijksoverheid.nl .
Zou jij kunnen kijken of de kamerbrief toereikend is of dat sommige vragen nog wel enige verheldering behoeven?
Groet,
5.1.2e

Van: 5.1.2e 5.1.2e < 5.1.2e @vpro.nl>
Verzonden: dinsdag 3 maart 2026 14:31
Aan: 5.1.2e , 5.1.2e < 5.1.2e @minjenv.nl>; 5.1.2e . - 5.1.2e < 5.1.2e @minjenv.nl>
Onderwerp: Vragen Argos (VPRO) over hack JIO via Citrix kwetsbaarheid

Beste 5.1.2e en 5.1.2e ,
Voor Argos (VPRO) doe ik onderzoek naar de gevolgen van de hack van de Justitiële ICT-Organisatie in de zomer van 2025.
Het NCSC stelde in augustus 2025 al vast dat er meerdere kritieke organisaties binnen Nederland succesvol aangevallen zijn via verschillende kwetsbaarheden in de Citrix NetScaler (CVE-2025-5349, CVE-2025-5777 en

CVE-2025-6543). Uit mijn onderzoek blijkt dat de Justitiële ICT-Organisatie (JIO) één van deze gehackte organisaties is, en dat de indringers bovendien toegang hadden tot de ICT-systemen van opdrachtgevers van JIO, waaronder het ministerie van Justitie en Veiligheid.
Ik wil zowel JIO als het ministerie van J&V enkele vragen over deze kwestie voorleggen. Kunnen jullie hier **uiterlijk op dinsdag 10 maart, 10:00 uur**, op reageren? Mochten er nog onduidelijkheden zijn, laat het me weten, dan licht ik een en ander toe.
Bij voorbaat hartelijk dank!

Vragen aan JIO

- Wij constateren dat kwaadwillende actoren in de zomer van 2025 hebben kunnen binnendringen bij JIO via een kwetsbaarheid in de Citrix Netscaler. Wat is daarop uw reactie?

- Op welke datum vond het eerste misbruik van deze kwetsbaarheid bij JIO plaats?

- Op welke datum constateerde JIO dat aanvallers misbruik hadden gemaakt van deze kwetsbaarheid bij JIO?

- Wij constateren dat door een configuratiefout in de firewall (die wordt beheerd door Solvinity) de monitoring en logging van de firewall uitstond. Hierdoor konden de indringers vanuit de demilitarized zone (DMZ) onopgemerkt doordringen tot de ICT-systemen van JIO en de klanten / opdrachtgevers van JIO. Wat is daarop uw reactie?

- Hoe kan het dat JIO niet doorhad dat de firewall verkeerd was geconfigureerd?

- Hoe lang stond die firewall al verkeerd geconfigureerd?

- Wat is het beleid van JIO ten aanzien van monitoring en logging? Voert JIO periodieke controles uit op de firewalls en andere vergelijkbare security-systemen?

- Wat weet JIO over de identiteit van de indringers? Klopt het dat de veiligheidsdiensten hebben gewaarschuwd dat het waarschijnlijk gaat om een statelijke actor?

- Welke informatie heeft JIO over deze ICT-inbreuk gedeeld met haar opdrachtgevers?

- Wat heeft JIO gedaan om te voorkomen dat gevoelige data gelekt zouden worden?

- Verschillende betrokkenen hebben gewaarschuwd voor de risico's van de hack en hebben JIO geadviseerd de ICT-systemen offline te halen. Wij constateren dat JIO dit niet heeft gedaan. Waarom heeft JIO dit advies niet opgevolgd?

- Verschillende bronnen wijzen op het risico dat enkelbanden niet meer (volledig) zouden functioneren als JIO offline zou gaan. Erkent u dit risico? Welke rol speelde dit risico in het besluit om de organisatie niet offline te halen? Weet u inmiddels of de enkelbanden in zo'n geval inderdaad niet meer (volledig) zouden functioneren?

- 5.1.2f heeft onderzoek gedaan naar aanleiding van de hack. Klopt het dat het (concept)rapport van 5.1.2f met u gedeeld is? Waarom is er nog geen definitief rapport? Waarom zijn de resultaten niet met de Tweede Kamer gedeeld?

- Wij concluderen dat de indringers die via het Citrix-lek zijn binnengekomen mogelijk nog steeds mee kunnen kijken in de systemen van JIO en de klanten van JIO. Kunt u uitsluiten dat de indringers nog steeds mee kunnen kijken?

- Uit onze bronnen blijkt dat 5.1.2e 5.1.2e 5.1.2e per 1 maart vertrokken is bij JIO. Waarom is hij vertrokken? Houdt zijn vertrek verband met de tekortschietende informatiebeveiliging van JIO?

Vragen aan J&V

- Was de minister van Justitie en Veiligheid in de zomer van 2025 op de hoogte dat JIO was gehackt via (een of meerdere) kwetsbaarheden in Citrix Netscalers? Zo ja, vanaf wanneer?

- Wij constateren dat aanvallers, die via de kwetsbaarheid in de Netscalers waren binnengedrongen tot de demilitarized zone (DMZ), door de verkeerde configuratie van de firewall van Solvinity toegang hadden tot zowel de ICT-systemen van opdrachtgevers van JIO, als tot andere klanten van Solvinity. Was de minister in de zomer van 2025 op de hoogte van falende firewall en de gevolgen daarvan? Zo ja, vanaf wanneer?
- JIO beheert ook (een deel van) de ICT van het ministerie van J&V. In hoeverre is J& V voor haar ICT afhankelijk van JIO?

- Wij concluderen dat de aanvallers via JIO / de verkeerd geconfigureerde firewall van Solvinity ook toegang had tot de ICT-systemen van J&V. Hoe schatte de minister de risico's hiervan in?

- Is de minister ingelicht over de – vermoedelijke – identiteit van de hackers? Klopt het dat de veiligheidsdiensten hebben gewaarschuwd dat het gaat om een statelijke actor?
- Was de minister betrokken bij het besluit van JIO om de ICT-systemen in nasleep van de hack niet offline te halen? Zo ja, waarom heeft de minister besloten de systemen niet offline te halen?

- Verschillende bronnen wijzen op het risico dat enkelbanden niet meer (volledig) zouden functioneren als JIO offline zou gaan. Erkent u dit risico? Welke rol speelde dit risico in het besluit om de organisatie niet offline te halen?
- Welke acties heeft het ministerie genomen om te voorkomen dat de indringers toegang zouden kunnen blijven houden tot de ICT-systemen van het ministerie en de andere opdrachtgevers van JIO? Kunt u uitsluiten dat de indringers nu geen toegang meer hebben tot deze systemen?

Met vriendelijke groet,

5.1.2e
journalist | radiomaker
argos | vpro
5.1.2e | 5.1.2e @vpro.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security