Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

26 643 **Informatie- en communicatietechnologie (ICT)**

24 587 **Justitiële Inrichtingen**

Nr. 1492

BRIEF VAN DE STAATSSECRETARISSEN VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 27 februari 2026

Met deze brief informeer ik uw Kamer over de aanvullende constateringen van misbruik van de kwetsbaarheden in Ivanti Endpoint Manager Mobile (EPMM) binnen de overheid die de staatssecretarissen van Justitie en Veiligheid en van Binnenlandse Zaken aankondigden in hun Kamerbrief van 6 februari 2026[1].

Ik heb binnen de overheid verder laten inventariseren welke organisaties gebruik maken van deze voorziening en of er aanwijzingen waren van misbruik. Bij de volgende overheidsorganisaties zijn sporen van misbruik gevonden of kon dit niet met voldoende zekerheid worden uitgesloten:

- Ministerie van Justitie en Veiligheid: Autoriteit Persoonsgegevens (AP), Dienst Justitiële Inrichtingen, Dienst Terugkeer & Vertrek, Justitiële ICT Organisatie en Raad voor de Rechtspraak;
- Ministerie van Volksgezondheid, Welzijn en Sport: het College ter Beoordeling van Geneesmiddelen;
- Eén gemeente.

De betreffende gemeente neemt op basis van haar zelfstandigheid alle benodigde stappen inclusief eventuele meldingen in de media.

Specifiek ten aanzien van DJI kan ik melden dat werkgerelateerde gegevens van medewerkers, zoals naam, zakelijk e-mailadres, telefoonnummer en locatiegegevens, zijn ingezien door onbevoegden. Nadat het incident is ontdekt, zijn direct maatregelen getroffen. Daarnaast zijn de medewerkers van DJI op de hoogte gebracht en voorzien van een handelingskader. Ik ben me zeer er van bewust welke impact deze situatie kan hebben op de medewerkers van DJI. Door DJI wordt mede daarom in gezamenlijkheid met partijen uit de keten nauwlettend in de gaten gehouden of en welke gevolgen het datalek heeft.

[1] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2026Z02656&did=2026D05964

kst-26643-1492
ISSN 0921 - 7371
's-Gravenhage 2026

Uiteraard hebben ook de andere organisaties waar mogelijk ongeautoriseerd (persoons)gegevens zijn ingezien aandacht voor de zorgen hierover bij de medewerkers. De betrokken organisaties hebben direct de nodige maatregelen getroffen. Ook hebben zij waar relevant hun medewerkers geïnformeerd, voorlopige meldingen gedaan bij de AP en aangifte bij de Politie.

Het Nationaal Cyber Security Centrum (NCSC) doet technisch onderzoek en vervult een coördinerende rol bij de uitwisseling van (technische) dreigings- en incidentinformatie via diverse kanalen. Daarbij onderhoudt het NCSC nauw contact met betrokken organisaties, hun incident response partijen, en (inter)nationale partners.

Vanzelfsprekend heeft dit onze volle aandacht en als daar aanleiding toe is kom ik uiteraard terug bij uw Kamer.

De Staatssecretaris van Binnenlandse Zaken,
E. van der Burg

De Staatssecretaris van Justitie en Veiligheid,
K.T. van Bruggen