26643 Informatie- en communicatietechnologie (ICT)

Nr. 1565 Brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 september 2026

Graag informeer ik u nader over een kwetsbaarheid in Citrix Netscaler waar ook de Rijksoverheid gebruik van maakt. Na geïnformeerd te zijn via een Europese partner, heeft het Nationaal Cyber Security Centrum (NCSC) op vrijdagmiddag 25 september jl. vertrouwelijk bedrijven en organisaties, waaronder de rijksoverheid, geïnformeerd en geadviseerd om tijdig passende maatregelen te nemen inzake twee ernstige kwetsbaarheden in Citrix Netscaler. Er was op dat moment nog geen patch beschikbaar, en de kwetsbaarheden werden al actief (buiten Nederland) misbruikt. In de dagen daarna heeft het NCSC geadviseerd wat te doen. Daarnaast heeft het NCSC op maandag 28 september aanvullend gedeeld hoe ze kunnen achterhalen of er sprake is van inbraak in systemen.

Citrix Netscaler zorgt ervoor dat websites en applicaties snel en betrouwbaar bereikbaar blijven. Dit wordt bijvoorbeeld gebruikt om thuiswerken te faciliteren. Medewerkers kunnen zo op afstand toegang krijgen tot het netwerk en de bedrijfsomgevingen van een organisatie. Citrix wordt bij de rijksoverheid breed gebruikt. Een inbraak op Citrix kan daarom grote impact hebben.

Het advies van het NCSC was om te overwegen om preventief de Citrix-voorzieningen af te koppelen van het internet. Hierbij dient een risicoafweging plaats te vinden, omdat Citrix soms gebruikt wordt in een primair proces dat door moet gaan. De CIO Rijk heeft daarom op zaterdag 26 september jl. de Rijksoverheid de lijn meegegeven ‘loskoppelen tenzij’. ‘Tenzij’ is van toepassing wanneer de impact op de primaire taken of op burgers en bedrijven onevenredig groot is.

De overheid heeft het dit advies van CIO Rijk tot het preventief loskoppelen breed toegepast. Citrix heeft zondagavond voor het eerst publiekelijk gecommuniceerd over de kwetsbaarheden, patches beschikbaar gemaakt waarmee deze kwetsbaarheden verholpen kunnen worden en voor het eerst informatie gegeven over hoe misbruik waargenomen kan worden. Organisaties worden aangemoedigd te onderzoeken of aanvallers zijn binnengedrongen, de patch te testen en deze zo snel als verantwoord toe te passen.

De Citrix-voorzieningen zijn nog niet in alle gevallen weer beschikbaar voor werken op afstand. Er wordt momenteel getest of de patch goed werkt en niet zelf leidt tot verstoringen. Daarnaast wordt er sporenonderzoek uitgevoerd. Waakzaamheid is geboden, omdat aanvallers hebben mogelijk de tijd hebben gehad zich in de systemen te nestelen. CIO Rijk adviseert daarom aan alle Rijksoverheidsorganisaties te onderzoeken of er sporen van inbraak zijn en de komende tijd waakzaam te zijn en te blijven. Het advies daarbij is om te handelen vanuit een ‘assume breach’-principe. Dit houdt in dat men er rekening mee moet

houden dat een aanvaller mogelijk al toegang heeft. Op basis van dit principe moeten maatregelen ingericht worden voor detectie om relevante sporen te behouden en verdere toegang te beperken.

Momenteel staan CIO Rijk en het NCSC in contact met meerdere Rijksoverheidspartijen die mogelijk getroffen zijn door deze kwetsbaarheden. Omwille van het onderzoek doe ik hierover geen nadere mededelingen. We houden de situatie nauwgezet in de gaten en monitoren de ontwikkelingen.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
E. van der Burg