Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

TER BESPREKING

Nota actief openbaar
Ja

Onze referentie
2023-0000556982

Datum
1 september 2023

Samengewerkt met
Kiesraad, CZW, Eigenaarsadvisering, CISO BZK

Bijlage(n)
1

Aan Minister van BZK
Van Team verkiezingen

nota

Melding beveiligingsrisico's OSV2020

Aanleiding

De Kiesraad heeft BZK geïnformeerd over een melding omtrent beveiligingsrisico's in OSV2020. De Kiesraad heeft gemeld dat de beveiligingsrisico's zijn opgelost.

De beveiligingsrisico's zijn gemeld door een externe partij, conform informeel geldende procedures rondom Coördinated Vulnerability Disclosure (CVD). De Kiesraad heeft gemeld voornemens te zijn op 8 september een bericht over deze melding op de website te zetten. Ook zal de externe partij een blog schrijven over deze casus.

Geadviseerd besluit

U wordt gevraagd kennis te nemen van deze nota en in te stemmen met het versturen van bijgevoegde brief om de Kamer over deze melding te informeren.

Kern

- De gemelde beveiligingsrisico's zijn opgelost.
- Nu de melding is opgelost stelt de Kiesraad voor om over te gaan tot berichtgeving over de melding. Dit is afgesproken met de melder.
- De Kiesraad heeft op dit moment geen indicaties dat de software is gemanipuleerd.
- Voorgesteld wordt gelijktijdig met de communicatie door de Kiesraad een brief aan de Tweede Kamer te sturen. In de Kamerbrief informeert u de Tweede Kamer feitelijk over de melding en dat deze is opgelost. Hierbij informeert u tevens de Kamer over welke maatregelen in het verkiezingsproces (reeds) zijn genomen om de betrouwbaarheid van de verkiezingsuitslag te borgen.

Toelichting

Wat is OSV2020

- OSV2020 is het softwareprogramma dat de Kiesraad ter beschikking stelt ter ondersteuning van het verkiezingsproces. OSV bestaat onder andere uit de volgende modules:
    - Een module voor politieke partijen ten behoeve van het opstellen van de documenten voor de kandidaatstelling.
    - Een module voor het centraal stembureau om de kandidatenlijsten vast te stellen

- Een module voor de gemeentelijk stembureaus, hoofdstembureaus, het nationaal briefstembureau en centraal stembureaus voor het optellen en vaststellen van de verkiezingsuitslag.

De melding

- De Kiesraad heeft op 28 juni een melding ontvangen over beveiligingsrisico's in de module voor politieke partijen in OSV2020.
- De beveiligingsexpert (een medewerker van het bedrijf Zerocopter) die deze melding heeft gedaan werkt niet voor de Kiesraad en heeft dit zelfstandig en zonder verzoek van de Kiesraad onderzocht.
- Dit onderzoek was mogelijk omdat de installatiesoftware van OSV2020 op de website van de Kiesraad staat, zodat politieke partijen de software vanaf daar kunnen downloaden.
- De Kiesraad meldt dat de kwetsbaarheden vermoedelijk niet eerder zijn aangetoond omdat bij beveiligingstesten de experts altijd hebben gekeken naar de software van OSV2020 zelf en niet naar de installatiesoftware. De gevonden beveiligingsrisico's stonden niet in de software, maar in de installatiesoftware. Vanaf nu wordt de installatiesoftware expliciet meegenomen in de scope van alle beveiligingstesten.

Gevolgen voor OSV2020 en de verkiezingen

- In Nederland stemmen we met papieren stembiljetten. Die worden met de hand geteld. OSV2020 is ondersteunend aan het proces bij de uitslagvaststelling. De papieren stembiljetten en processen-verbaal zijn leidend.
- Bij de uitslagvaststelling van een verkiezing worden handmatige steekproefcontroles uitgevoerd of OSV2020 correct heeft gewerkt. Ook worden alle optellingen die uit OSV2020 komen openbaar gemaakt, zodat iedereen kan controleren of deze optellingen correct zijn gedaan. Deze transparantie en controleerbaarheid zijn belangrijke waarborgen tegen manipulatie van OSV2020.
- De beveiligingsmelding had betrekking op installatiesoftware van de module voor politieke partijen. De formele documenten in de kandidaatstellingsprocedure worden door het centraal stembureau gecontroleerd voordat de kandidatenlijst wordt opgemaakt.

De beveiligingsrisico's:

- In de bijgeleverde installatiesoftware van OSV2020 bleken inloggegevens van applicaties te staan die de leverancier van OSV gebruikt.
- Een van de inloggegevens kon worden gebruikt om toegang te verkrijgen tot een server die vanaf het internet te bereiken is. Op deze server zet leverancier alle software die "af" is klaar voor klanten om deze te downloaden en vervolgens verder te verspreiden. Deze software wordt digitaal ondertekend met een zogenaamde private sleutel.
- Een andere kwetsbaarheid die in de installatiesoftware stond was het pad naar deze private sleutel op het interne netwerk van de leverancier en tevens de gebruikersnaam en wachtwoord om bij deze sleutel te komen.

Nieuwe beveiligingstesten voor de TK-verkiezing

- Bij elke verkiezing laat de Kiesraad de module uitslagvaststelling van OSV2020 toetsen. Hierbij wordt gecontroleerd of OSV2020 correct volgens de Kieswet werkt. Daarnaast wordt de beveiliging van OSV2020 getest. Dit gebeurt door externe onafhankelijke partijen die elkaar afwisselen in een roulatiesysteem. Hoe dit ingevuld wordt is vastgelegd bij de aanbesteding van de opdracht voor deze toetsen. Bij deze Tweede Kamerverkiezing worden deze toetsen door KPMG en HackDefense uitgevoerd.

- Na het oplossen van de gemelde beveiligingsrisico's heeft de Kiesraad opnieuw beveiligingstesten laten uitvoeren door HackDefense.
- De Kiesraad heeft gemeld dat de bevindingen van HackDefense reeds zijn opgelost in de versie van OSV2020 die nu beschikbaar wordt gesteld aan politieke partijen ten behoeve van de kandidaatstellingsprocedure voor de aankomende Tweede Kamerverkiezing.
- Voor de module uitslagvaststelling van OSV2020 geldt dat de Kiesraad heeft gemeld in aanloop naar de Tweede Kamerverkiezing extra beveiligingstesten (pentesting en code review) uit te voeren, met expliciet het meenemen van de installatiesoftware.
- Het is de verwachting dat de uitkomsten van deze onderzoeken uiterlijk op 9 oktober openbaar worden (*dit is een wettelijke termijn)*.
- Uit het onderzoek door HackDefense komt het volgende naar voren:
    - HackDefense is over het geheel genomen positief over de beveiliging van de applicatie. Er is duidelijk aandacht besteed aan de veiligheid. Wel zijn er twee belangrijke verbeterpunten:
        - Er is een functie gevonden die ooit ontwikkeld is, maar niet actief gebruikt wordt voor verkiezingen. Deze zat als het ware "weggestopt", maar kon nog wel worden gebruikt. Deze bleek het uploaden van onveilige bestanden toe te staan. Daarmee ontstaat het risico op ongeautoriseerde toegang tot de software.
        - De software maakt een gebruikersaccount aan in Windows, met een wachtwoord dat door anderen te herleiden is. Daardoor zou een aanvaller kunnen inloggen op de computer waarop de software geïnstalleerd is. Hiervoor is een ander type account veiliger, te weten een service account.

- Daarnaast doet HackDefense nog zes aanbevelingen die geen, of slechts een klein, risico oplossen, maar die naar hun mening wel een verbetering zouden zijn

Politieke context
In aanloop naar de Tweede Kamer is het waarschijnlijk dat deze casus aanleiding kan zijn voor vragen vanuit de Tweede Kamer over de betrouwbare werking van OSV2020 in het licht van de recent gestopte ontwikkeling van het Digitaal Hulpmiddel Verkiezingen (DHV) dat OSV2020 zou moeten vervangen.

Op dit moment is de Wet programmatuur verkiezingsuitslagen in behandeling bij de Tweede Kamer. Met dit wetsvoorstel worden de taken, verantwoordelijkheden en bevoegdheden in het beheer en gebruik van de uitslagprogrammatuur in het verkiezingsproces (op dit moment OSV2020) in de Kieswet verder vastgelegd.

Communicatie
De Kiesraad verwacht op maandag 11 september een nieuwsbericht over deze casus op zijn website te plaatsen. Beoogde verzending van de kamerbrief is gelijktijdig.

Informatie die niet openbaar gemaakt kan worden

Motivering
In de openbaar gemaakte versie van deze nota zijn alle persoonsgegevens van ambtenaren geanonimiseerd. Hiernaast kan bedrijfsgevoelige informatie niet worden openbaargemaakt.

Bijlagen

Volgnummer	**Naam**	**Informatie**
1	Brief aan Tweede Kamer	