FOX IT
part of nccgroup

CLASSIFICATIE
OPENBAAR

OSV-2020 Software Penetration Test

U module voor de Europese verkiezingen

Datum	March 22, 2024
Referentie	PR-230511
Opdrachtgever	Kiesraad
Versie	1.0

FOR A MORE SECURE SOCIETY

1 Documentclassificatie

Dit document is geclassificeerd als OPENBAAR.

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 Box 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

Managementsamenvatting

In opdracht van de Kiesraad heeft Fox-IT een technisch beveiligingsonderzoek (penetratietest) uitgevoerd op de Ondersteunende Software Verkiezingen 2020 (OSV-2020) software die wordt gebruikt ter ondersteuning van de uitslagvaststelling van de Europese verkiezing. Het doel van het onderzoek was het identificeren van kwetsbaarheden in de software waarmee kwaadwillende partijen invloed zouden kunnen uitoefenen op het verkiezingsproces.

De reikwijdte van het onderzoek van de penetratietest van dit rapport was beperkt tot de Uitslagen (U) module van de OSV-2020 software. De politieke partijen module (PP) en de kandidaatstelling module (KS) van de OSV-2020 software zijn eerder getest en het resultaat daarvan bevindt zich in een eerder losstaand rapport. Het gebruik van Multi Factor Authenticatie, airgap bypass mogelijkheden en nog een aantal testonderdelen zijn na afweging van de Kiesraad, expliciet buiten de reikwijdte van het onderzoek geplaatst, en zijn daarom geen onderdeel van dit rapport. Organisatorische elementen van de Kiesraad zelf, zoals fysieke toegang, het netwerk waar de software zich op bevindt, of het phishen van medewerkers zijn ook expliciet buiten de reikwijdte van het onderzoek geplaatst door de Kiesraad. Een uitgebreide lijst van onderdelen die buiten de reikwijdte van het onderzoek zijn geplaatst, is te vinden in het Onderzoek Details hoofdstuk van dit rapport.

Gedurende de timeboxed[1] penetratietest heeft Fox-IT verschillende kwetsbaarheden en misconfiguraties gevonden die van invloed zijn op de U module van de OSV-2020 software. Hieruit blijkt dat er mogelijk een aanvalspad is waarmee een aanvaller de verkiezingsdefinities of de kandidatenlijst in de U module zou kunnen beïnvloeden. Dit betreft een pad bestaat uit een combinatie van social engineering, door invalide data aan te leveren, en digitale controle die niet afdoende is om dit af te vangen. Echter, acht Fox-IT de kans op misbruik van het geschetste aanvalspad zeer onwaarschijnlijk vanwege de volgende redenen die door de Kiesraad mondeling zijn toegelicht:

- Hoewel het in theorie mogelijk is om de verkiezingsdefinities of de kandidatenlijst binnen de U module van de OSV-2020 software aan te passen, levert dit op een later moment problemen op bij het invoeren van stemdata in de U module, door het ontbreken van de juiste velden, waardoor incorrecte doorvoer eerder opvalt.
- Er zijn veel handmatige validatieslagen van papieren documenten. Indien correct uitgevoerd, zal bij het ontbreken van afdoende digitale controle in de U module van de OSV-2020 software, de handmatige validatieslag dit probleem afvangen.
- Er is bij dit aanvalspad een ontbrekende stap, waardoor het volledig pad momenteel enkel theoretisch blijft en praktisch niet uit te voeren is.

Verder zijn er een aantal andere bevindingen gedaan, die doorgaans makkelijk met andere bevindingen te combineren zijn, maar waarbij momenteel de vervolgstap ontbreekt. Denk hierbij aan het kunnen uploaden van malafide data en scripts, waarbij de uitvoer van het script of het ophalen van malafide data nog ontbreekt, of het enumereren van gebruikersnamen, die slechts een onderdeel zijn van de inlogprocedure.

[1] Fox-IT kan uitsluitend bevindingen rapporteren die zijn gedaan binnen de periode van onderzoek, en alleen voor zover zaken zijn gevonden binnen de beperkingen van de maximale duur van de opdracht. Ondanks onze maximale inspanning is het altijd mogelijk dat er nog meer kwetsbaarheden bestaan dan die Fox-IT heeft gevonden en gerapporteerd.

Tot slot is er onderzoek verricht naar het gebruik van onversleutelde wachtwoorden die voor misbruik vatbaar zijn, inclusief de mogelijkheid dat deze worden gebruikt in data die door de gebruikte programmeertaal (Java) is omgezet in een geserialiseerd formaat. Er zijn tijdens het onderzoek geen onversleutelde wachtwoorden gevonden die daadwerkelijk door de U module van de OSV-2020 software gebruikt worden.

Uit het onderzoek zijn zeven bevindingen geconstateerd, welke gedocumenteerd zijn in deze rapportage. Geen van de bevindingen hebben de risicoclassificatie kritiek of hoog. Wel zijn er twee bevindingen met een gemiddeld risico en vijf met een lage risicoclassificatie. Van het totale aantal bevindingen is er één aangemerkt als een bevinding waarbij Fox-IT aanraadt deze met prioriteit te verhelpen, omdat het een aanvaller in staat stelt om aanzienlijke vooruitgang te boeken bij het compromitteren van de OSV-2020-U software. Het verhelpen van deze bevinding zou daarom de beveiliging van de OSV-2020-U software aanzienlijk moeten verhogen. Een overzicht hiervan is hieronder gevisualiseerd:

Kritiek	Hoog	Gemiddeld	Laag
0	0	2	5

Op basis van dit onderzoek geeft Fox-IT de volgende aanbevelingen:

- Verbeter de baseline hardening van de U module;
- Verbeter de input en output filtering van gebruikersinput binnen de U module;
- Verbeter de digitale verificatie van de invoer van bestanden, met betrekking tot zowel stemdata als benodigde meta data voor de uitvoer van de U module;
- Overweeg additionele testtijd toe te wijzen bij toekomstige penetratietesten om verborgen functionaliteit verder te onderzoeken.

Deze aanbevelingen worden nader beschreven in het hoofdstuk]Strategische Aanbevelingen.

Samenvattend, op basis van het onderzoek concludeert Fox-IT dat hoewel er verschillende bevindingen zijn vastgesteld in de U module van de OSV-2020 software en additionele testtijd wenselijk was, de kans op het uitoefenen van invloed op de verkiezing middels enkele technische stappen via de U module zeer onwaarschijnlijk is. Daarnaast maakt de handmatige validatieslag van het fysiek controleren van de papieren documenten die tijdens het verkiezingsproces worden gebruikt, de kans op mogelijk invloed op de verkiezing nog kleiner.

2 Inhoudsopgave

1 Documentclassificatie **2**

2 Inhoudsopgave **5**

3 Onderzoek Details **6**
3.1 Rapportagetaal . . . 6
3.2 Onderzoeksvraag . . . 6
3.3 Onderzoeksreikwijdte . . . 6
3.3.1 Testonderdelen buiten de onderzoeksreikwijdte . . . 7
3.4 Onderzoeksaanpak . . . 7
3.4.1 Automatisch scannen . . . 8
3.4.2 Applicatie in kaart brengen . . . 8
3.4.3 Technische kwetsbaarheidstests . . . 8
3.4.4 Tests van bedrijfslogica . . . 8
3.5 Creatief Proces . . . 9
3.6 Toegewezen Tijd voor Penetratietest . . . 9
3.7 Beperkingen & Voorbehouden . . . 9

4 Onderzoeksconclusies **10**

5 Strategische Aanbevelingen **12**

6 Risicocorrelatie **14**

7 Bevindingsdefinities **15**

8 Overzicht bevindingen **16**

9 Technishe Bevindigen **17**
Bevinding 1: CSRF & CSP Bypass . . . 17
Bevinding 2: Weak User Password Policy . . . 20
Bevinding 3: Signature on Voting Data can not be Verified Using a Chain of Trust . . . 22
Bevinding 4: Verification Check of the Import of the Election Definitions can be Improved . . . 24
Bevinding 5: Log Contains Full Hash of the Verification Check of the Import of Election Candidate List . . . 26
Bevinding 6: Enumeration of Blocked Accounts is Possible . . . 28
Bevinding 7: Import of the Election Definitions can be Abused to Store any File Persistently . . . 30

3 Onderzoek Details

3.1 Rapportagetaal

Het rapport is in het Nederlands geschreven, op de technische bevindingen na, welke in het Engels zijn verwoord. De reden van het gebruik van de Engelse taal is dat deze technische bevindingen zo makkelijk met betrokken partijen gedeeld kunnen worden en omdat hiermee voorkomen wordt dat technische termen in het Engels in onduidelijk verwoord Nederlands vertaald worden. Deze duidelijkheid kan vervolgens weer bijdragen aan het snel oplossen van de bevindingen uit dit rapport.

3.2 Onderzoeksvraag

Namens de Kiesraad heeft Fox-IT een technische beveiligingsbeoordeling (penetratietest) uitgevoerd op de OSV-2020 software die wordt gebruikt om de uitslagvaststelling voor de Europese verkiezingen te ondersteunen. Het doel van het onderzoek was om kwetsbaarheden te identificeren die kwaadwillenden zouden kunnen uitbuiten om het verkiezingsproces te beïnvloeden. Meer specifiek probeerde Fox-IT de volgende onderzoeksvragen te beantwoorden:

- Welke technische kwetsbaarheden kan Fox-IT identificeren in de Uitslagen (U) module van de OSV-2020 software?
- Welk risiconiveau kent Fox-IT toe aan elke bevinding?
- Wat zijn de belangrijkste oorzaken van de gevonden kwetsbaarheden?
- Hoe kan de Kiesraad eventuele ontdekte kwetsbaarheden verhelpen en gerelateerde risico's verder beperken?
- Bevat de U-module van de OSV-2020 software hardgecodeerde wachtwoorden of ander gevoelig materiaal zoals cryptografische sleutels?
- Is het mogelijk voor kwaadwillenden om de resultaten van de Europese verkiezingen te beïnvloeden door middel van de U-module in de OSV-2020 software?

3.3 Onderzoeksreikwijdte

De onderzoeksreikwijdte van de penetratietest was beperkt tot de U-module van de OSV-2020 software. Organisatorische elementen van de Kiesraad zelf, zoals fysieke toegang, het netwerk waarop de software zich bevindt, of phishing van medewerkers waren expliciet buiten de reikwijdte van het onderzoek. Voor de volledigheid volgt een overzicht van alle OSV-2020 modules. Elke individuele OSV-2020 module heeft een aparte taak en kan als volgt worden samengevat:

- De U-module is de module die wordt gebruikt voor het verwerken van stemuitslagen. Met behulp van deze module kunnen de telresultaten van ondergeschikte kiesorganen worden getotaliseerd en uiteindelijk gebruikt worden om de zetelverdeling te berekenen;

- De KS-module is een module die door de Kiesraad wordt gebruikt om de kandidaatstellingsprocedure te ondersteunen. Het heeft onder andere een verbinding met de Basisregistratie Personen (BRP). Daarom wordt de KS-module lokaal geïnstalleerd bij de Kiesraad op een privénetwerk tijdens de verkiezingen. De penetratietest voor de KS-module heeft los van deze test plaatsgevonden en wordt beschouwd als buiten de reikwijdte van het onderzoek;

- De PP-module is de module die door politieke partijen wordt gebruikt om hun kandidatenlijsten samen te stellen en in te dienen. Partijen, evenals burgers, kunnen deze module downloaden van de Kiesraad-website en installeren op hun eigen systeem. Het apparaat waarop de PP-module is geïnstalleerd, kan verbonden zijn met het internet. De penetratietest voor de PP-module heeft los van deze test plaatsgevonden en wordt beschouwd als buiten de reikwijdte van het onderzoek.

Om de test uit te voeren, heeft de Kiesraad Fox-IT voorzien van verschillende ZIP-bestanden met de installatiebestanden die nodig zijn om de OSV-2020-U applicatie op de eigen machines van Fox-IT te installeren. De SHA256-hashes voor de ontvangen bestanden zijn als volgt:

Filename	SHA256 hash
2024-01-12_WAS_1.10.2.1.zip	46E6CBE5F359CC8FE56B29601ED3BCB3DF0DE76BDD6DFB99064BEC1B74D39A5E
Properties_Metadata_EP2024.zip	1909B6BA7A2238FBCED18C7C8CC2AE7860A8F1E8147FC3664F92080EB7998D98

3.3.1 Testonderdelen buiten de onderzoeksreikwijdte

De politieke partijen module (PP) en de kandidaatstelling module (KS) van de OSV-2020 software zijn eerder getest en het resultaat daarvan bevindt zich in een eerder losstaand rapport.

Verder zijn het gebruik van Multi-Factor Authenticatie, airgap bypass-mogelijkheden en nog een aantal testonderdelen na gegronde afweging door de Kiesraad expliciet buiten de reikwijdte van het onderzoek geplaatst en zijn daarom geen onderdeel van dit rapport.

In totaal zijn de volgende testonderdelen expliciet buiten de reikwijdte van het onderzoek geplaatst:

Werkt zoals ontworpen:

- Omzeilen van airgap detectie tijdens installatie van de OSV-2020-U software.
- Omzeilen van airgap detectie tijdens de uitvoer van de OSV-2020-U software.

Niet relevant door korte duur van het bestaan van het netwerk (enkele dagen rond de verkiezing):

- Factor Authenticatie
- “Hostname” in cookies die door de U-module in gebruik zijn
- Het gebruik van de permission policy en referrer policy HTTP security headers binnen de OSV-2020-U applicatie.

3.4 Onderzoeksaanpak

Elke applicatie is anders en vereist dus een andere aanpak. Ondanks de verschillen is de methodologie van het testen een min of meer dezelfde gestructureerde aanpak zoals beschreven in de onderstaande paragrafen. Sommige van de hieronder beschreven acties kunnen parallel aan andere acties worden uitgevoerd.

3.4.1 Automatisch scannen

Elke applicatie wordt door de penetratietesters zowel aan een poort- als kwetsbaarheidsscans onderworpen, met applicaties zoals Nmap[2] om open poorten te beoordelen, Burp Suite[3] voor directe interactie met de webserver en Nuclei[4] om veelvoorkomende kwetsbaarheden in componenten van derden te ontdekken. Alle tools worden ingezet om automatisch te bepalen hoe groot het aanvalsoppervlak is binnen de onderzo eksreikwijdte van het onderzoek. De resultaten van deze geautomatiseerde controles worden geverifieerd om ervoor te zorgen dat er geen onterechte bevindingen worden gerapporteerd en om te controleren of de gerapporteerde kwetsbaarheden op een zinvolle manier kunnen worden misbruikt. Daarnaast kunnen specifieke URL's of functies worden ingediend voor verdere, meer precieze (geautomatiseerde) controles zodra ze zijn geïdentificeerd tijdens de beoordeling.

3.4.2 Applicatie in kaart brengen

Om alle functionaliteit van de applicatie en de mogelijke impact van geïdentificeerde problemen goed te kunnen beoordelen, brengen de penetratietesters eerst de functionaliteit van de applicatie in kaart. Dit proces houdt in dat de penetratietesters de applicatie gebruiken zoals deze bedoeld is, en webcrawlsoftware gebruiken zoals de eerder genoemde Burp Suite en Katana[5] om een gedetailleerder inzicht te krijgen in welke functionaliteit beschikbaar is voor een aanvaller. Tijdens deze stap noteren de penetratietesters elk opmerkelijk applicatiegedrag dat verder in de beoordeling kan worden gebruikt.

Daarnaast worden alle door de Kiesraad aangeleverde ZIP-bestanden met de gebouwde software uitgepakt en de Java-code gedecompileerd. Dit wordt gedaan in een poging om verborgen aanvalsvectoren te ontdekken die misschien niet aan de gebruiker worden getoond, maar desondanks aanwezig zijn. Deze informatie wordt vervolgens gebruikt om de lijst van gevonden functionaliteit verder aan te vullen, waarna de initiële fase van applicatiemapping wordt herhaald om ervoor te zorgen dat zoveel mogelijk eindpunten worden geanalyseerd.

Tot slot, na het uitpakken van alle aangeleverde code, zoekt Fox-IT naar de aanwezigheid van zwakke of standaardwachtwoorden, cryptografisch materiaal of andere mogelijk gevoelige gegevens die in de install atiebestanden en onderliggende code zijn ingebed.

3.4.3 Technische kwetsbaarheidstests

Zodra de applicatie in kaart is gebracht, gaan de penetratietesters verder met het manipuleren van de applicatiegegevens om kwetsbaarheden te identificeren, onder andere die in de OWASP top 10.[6] Deze omvatten kwetsbaarheden zoals SQL-injecties of commando-injectie, Cross Site Scripting (XSS), XML External Entity-injectie (XXE), onveilige deserialisatie en het lekken van gevoelige informatie. Het identificeren van deze kwetsbaarheden wordt zowel geautomatiseerd als handmatig uitgevoerd om ervoor te zorgen dat er geen onterechte kwetsbaarheden worden gerapporteerd. Vooral gevoelige functies binnen de applicatie worden nadrukkelijk handmatig getest om maximale controle te garanderen tijdens het testen.

3.4.4 Tests van bedrijfslogica

Een belangrijk onderdeel van elke webapplicatieonderzoek is het testen van bedrijfslogica. Deze tests worden uitgevoerd om te verifiëren of de applicatie veilig is ontworpen en niet op manieren kan worden gebruikt die niet door de ontwikkelaar zijn bedoeld. Voorbeelden hiervan zijn onjuiste toegangscontroles en het manipuleren van de achterliggende verificatieprocessen van een applicatie. Dergelijke verificaties vereisen kennis van de applicatie en kunnen daarom voornamelijk handmatig goed worden getest.

[2] Nmap de Network Mapper & Kwetsbaarheden Scanner: https://nmap.org/
[3] Burp Suite Pro: https://portswigger.net/burp/pro
[4] Nuclei Kwetsbaarheden Scanner: https://nuclei.projectdiscovery.io/
[5] Katana Web Crawler: https://github.com/projectdiscovery/katana
[6] OWASP top tien project: https://owasp.org/www-project-top-ten/

3.5 Creatief Proces

Het penetratietesten is en blijft een creatief proces. Ondanks dat er zo compleet mogelijk wordt getest met behulp van een gestructureerde aanpak, zijn er beperkingen. Deze beperkingen hangen samen met de creatieve aard van het werk, de beschikbare tijd, en de publieke kennis van specifieke kwetsbaarheden en aanvalstechnieken op het moment van testen. Daarom is het mogelijk dat niet alle beveiligingsrisico's worden ontdekt.

3.6 Toegewezen Tijd voor Penetratietest

In totaal was per penetratietester gemiddeld vier en een halve dag voor testen en twee dagen voor rapportage toegewezen. De penetratietest werd uitgevoerd door twee penetratietesters tussen 14 februari 2024 en 23 februari 2024. Fox-IT acht de beschikbare tijd voor testen en rapportage onvoldoende voor de gehele testomvang. Ondanks dat extra tijd de voorkeur heeft, blijven de algemene conclusies onveranderd.

3.7 Beperkingen & Voorbehouden

Tijdens het uitvoeren van de penetratietest identificeerde Fox-IT verschillende onderdelen waar meer onderzoekstijd wenselijk zou zijn, zoals de zekerheid van de digitale integriteit van de installatie bestanden en de risico's met betrekking tot door het proces verborgen onderdelen van de OSV-2020-U applicatie ,[7] die echter niet binnen de toegewezen testtijd grondig konden worden onderzocht.

Dit werd veroorzaakt door drie primaire redenen:

- De U-module bevat tienduizenden .java en honderden .xhtml (server-side HTML-sjabloncode) bestanden.[8] Fox-IT was niet in staat om elk bestand grondig te analyseren vanwege het feit dat Kiesraad minder tijd had toegewezen dan aanvankelijk door Fox-IT was gevraagd.
- Aangezien de applicatie door een Duitse organisatie is ontwikkeld, is de onderliggende code geschreven in een mix van Duits, Nederlands en Engels, waarbij het grootste deel van de code in het Duits is geschreven. Hierdoor vertraagde de taalbarrière de codeanalyse aanzienlijk voor onderzoekers die het Duits niet als moedertaal hebben.
- De aanvraag van het onderzoek heeft door de drukte in de planning van Fox-IT helaas een ongebruikelijk lange doorlooptijd gekend, in combinatie met de benodigde deadline van de Kiesraad resulteerde dit in een korter tijdsbestek voor de planning en uitvoering van het onderzoek.

Om grondiger onderzoek in de toekomst mogelijk te maken, adviseert Fox-IT de Kiesraad een uitgebreidere penetratietest met meer tijd uit te voeren voordat de software weer ingezet wordt voor een andere verkiezing dan de Europese.

[7] In de context van de OSV-2020-U applicatie verwijst de term "verborgen onderdelen" naar functies die beschikbaar of onbeschikbaar worden als gevolg van het vereiste proces van de applicatie. Dit is begrijpelijk gezien de functionaliteit van de OSV-2020-U, maar het resulteert in een vertraging en complicatie van het testproces.

[8] Deze statistieken sluiten code uit van bibliotheken van derden. Fox-IT heeft zijn best gedaan om eventuele dubbele jar-bestanden uit te sluiten en heeft alleen jar-bestanden opgenomen die beginnen met het voorvoegsel nl-vwp, *nl-wus*, en elect-*.

4 Onderzoeksconclusies

Fox-IT heeft een technische beveiligingsbeoordeling (penetratietest) uitgevoerd op de U-module van de OSV-2020 software die wordt gebruikt ter ondersteuning van het verkiezingsproces van de Europese verkiezingen. Het doel van deze beoordeling was om kwetsbaarheden te identificeren die kwaadwillende partijen zouden kunnen gebruiken om het verkiezingsproces te beïnvloeden. Deze test onthulde verschillende problemen met de beveiliging van de U-module van de OSV-2020 software. Het hoofdstuk "Onderzoek Details" documenteert de bevindingen van dit rapport in detail.

Gedurende de timeboxed[9] penetratietest heeft Fox-IT verschillende kwetsbaarheden en misconfiguraties gevonden die van invloed zijn op de U-module van de OSV-2020 software. Hieruit blijkt dat er mogelijk aanvalspaden zijn waarmee een aanvaller de verkiezingsdefinities of de kandidatenlijst in de U-module zou kunnen beïnvloeden. Dit betreft voornamelijk paden die een combinatie zijn van social engineering, door invalide data aan te leveren, en digitale controle die niet afdoende is om dit af te vangen. Echter, acht Fox-IT de kans op misbruik hiervan zeer onwaarschijnlijk vanwege de volgende redenen die door de Kiesraad mondeling zijn toegelicht:

- Hoewel het in theorie mogelijk is om de verkiezingsdefinities of de kandidatenlijst binnen de U-module van de OSV-2020 software aangepast door te laten voeren, levert dit op een later moment hoogst waarschijnlijk problemen op bij het doorvoeren van stemdata, door het ontbreken van de juiste velden, waardoor incorrecte doorvoer eerder opvalt.
- Er is veel controle[10] op papier. Indien correct uitgevoerd, zal bij het ontbreken van afdoende digitale controle, de papieren controle dit probleem ook afvangen.

Er is daarnaast een aantal bevindingen gedaan, die een eerste stap van een aanvalspad mogelijk maken, maar waarbij de vervolgstap ontbreekt. Denk hierbij aan het kunnen uploaden van malafide data en scripts, waarbij de uitvoer van de script of het ophalen van malafide data nog ontbreekt, of het enumereren van gebruikersnamen, die slechts een onderdeel zijn van de inlogprocedure.

Tot slot is er onderzoek verricht naar het gebruik van onversleutelde wachtwoorden die voor misbruik vatbaar zijn, inclusief de mogelijkheid dat deze worden gebruikt in data die door de gebruikte programmeertaal (Java) is omgezet in een geserialiseerd formaat. Er zijn tijdens het onderzoek geen onversleutelde wachtwoorden gevonden die daadwerkelijk door de U module van de OSV-2020 software gebruikt worden.

[9] Fox-IT kan uitsluitend bevindingen rapporteren die zijn gedaan binnen de periode van onderzoek, en alleen voor zover zaken zijn gevonden binnen de beperkingen van de maximale duur van de opdracht. Ondanks onze maximale inspanning is het altijd mogelijk dat er nog meer kwetsbaarheden bestaan dan die Fox-IT heeft gevonden en gerapporteerd.

[10] Volgens de Kiesraad wordt er een handmatige validatiecontrole uitgevoerd op de nauwkeurigheid van de fysieke lijst van kandidaten, die vervolgens wordt ondertekend door de betreffende politieke partij. De Kiesraad heeft aangegeven dat het fysieke document altijd leidend is. Fox-IT gaat ervan uit dat dit proces volgens de procedure verloopt.

Op basis van de verschillende problemen die tijdens de beoordeling zijn geïdentificeerd, in combinatie met de reikwijdte van de compromittering, kwam Fox-IT tot de volgende conclusies met betrekking tot de OSV-2020 software:

De OSV-2020 U-module is onvoldoende gehard De OSV-2020 U-module kan op meerdere punten veiliger afgesteld worden. Zo is momenteel het gebruikte wachtwoordbeleid te zwak geconfigureerd, is het nog mogelijk om geblokkeerde accounts te enumereren, maakt de OSV-2020-U-applicatielog het de gebruiker te makkelijk om de verificatie van het importeren van kandidatenlijst over te slaan en is het mogelijk de verificatie van het importeren van de verkiezingsdefinities volledig blind te accepteren. Het niet veiliger afstellen van OSV-2020-U applicatie maakt het momenteel makkelijker voor een aanvaller om een poging te doen het verkiezingsproces te beïnvloeden of te verstoren.

De OSV-2020 U-module filtert gebruikersinvoer onvoldoende Het gebrek aan invoerfiltering wordt gedetailleerd in bevindingen zoals het omzeilen van CSRF bescherming en de CSP HTTP beveiligings-header en het misbruiken van het importeren van de verkiezingsdefinities voor het persistent opslaan van willekeurige bestanden. Het gebrek aan een goede filtering van gebruikersinvoer maakt dergelijke bevindingen mogelijk. Deze kunnen misbruikt worden om de verschillende principes van vertrouwelijkheid, integriteit en beschikbaarheid van de applicatie en de gegevens die het bevat te ondermijnen.

De OSV-2020 U-module mist het gebruik van een vertrouwensketting (chain of trust) bij de invoer van stemdata Het niet gebruiken van een vertrouwensketting (chain of trust) bij de invoer van stemdata, maakt het voor gebruikers van de OSV-2020-U applicatie onmogelijk om te controleren of het ontvangen sleutelmateriaal geldig is. Doordat het sleutelmateriaal zelf niet op authenticiteit gecontroleerd kan worden, is digitale verificatie onvolledig. Hierdoor zal de gebruiker van de OSV-2020-U applicatie moeten terugvallen op een foutgevoeligere papieren controle.

5 Strategische Aanbevelingen

Dit hoofdstuk beschrijft de strategische aanbevelingen die de Kiesraad in staat zal stellen het algemene beveiligingsniveau te verhogen. Aanbevelingen voor individuele bevindingen met betrekking tot de OSV-2020-U software zijn te vinden in de overeenkomstige delen binnen het hoofdstuk Technische Bevindingen. Fox-IT raadt de Kiesraad aan een overkoepelend programma op te zetten, waarin individuele bevindingen worden toegewezen aan een verantwoordelijke.

Operationele bedrijfsvereisten kunnen aanleiding geven tot het accepteren van risico's (of gedeeltelijk accepteren), in plaats van deze te mitigeren. Wanneer Kiesraad besluit tot het (gedeeltelijk) accepteren van risico's, dan bevelen best practices aan dat deze beslissing op passende wijze wordt gedocumenteerd binnen een relevant Risicoregister. Middels het Risicoregister houdt de organisatie volledig zicht op het risico waaraan zij blootgesteld is. Aangezien de bedrijfsvoering van de Kiesraad geen onderdeel is van dit onderzoek, is het onbekend of zo'n Risicoregister al in gebruik is. Mocht de Kiesraad nog geen risicoregister hebben, dan raadt Fox-IT aan om een risicoregister in gebruik te gaan nemen.

Bij het beslissen hoe om te gaan met een bevinding, is het cruciaal om de onderliggende oorzaken aan te pakken in plaats van alleen de specifieke gevallen van de geïdentificeerde kwetsbaarheden. De onderliggende oorzaken die tijdens deze beoordeling zijn geïdentificeerd, zijn:

- De OSV-2020 U-module is onvoldoende gehard.
- De OSV-2020 U-module filtert gebruikersinvoer onvoldoende.
- De OSV-2020 U-module mist het gebruik van een vertrouwensketting (chain of trust).

Naast deze onderliggende oorzaken beveelt Fox-IT aan om extra testtijd toe te wijzen voor verdere onderzoeken. Verder raadt Fox-IT aan om deze onderzoeken enkele maanden van tevoren aan te vragen.

De OSV-2020 U-module is onvoldoende gehard Verschillende geïdentificeerde problemen komen voort uit suboptimale configuraties van de OSV-2020-software. Herstelacties die als gevolg van deze suboptimale configuraties zijn ondernomen, moeten worden beoordeeld tegen de veilige bouwstandaarden en impleme ntatieprocedures van de organisatie. Vervolgens moeten deze bouwstandaarden en implementatieprocedu res waar nodig worden bijgewerkt of zelfs volledig vervangen worden, om veilige afstelling van configuratie in de toekomst te kunnen waarborgen.

Om het basisniveau van de beveiliging te verbeteren, is het raadzaam om best practices die gebaseerd zijn op vrij toegankelijke richtlijnen en benchmarks te raadplegen en deze te integreren in de organisatorische richtlijnen. Voorbeeldveiligheidsbenchmarks voor zowel besturingssystemen als serversoftware zijn hier te vinden:

- https://www.cisecurity.org/cis-benchmarks/

De OSV-2020 U-module filtert gebruikersinvoer onvoldoende Bij het ontwikkelen van een applicatie is het verstandig om altijd aan te nemen dat gebruikers kwaadaardige gegevens zullen invoeren. Daarom moet voldoende aandacht worden besteed aan elke functionaliteit die omgaat met gebruikersinvoer en standaard moet alle invoer die niet is gespecificeerd worden afgewezen. De volgende bronnen bieden aanvullende informatie voor de verschillende filteringkwesties die tijdens de beoordeling zijn waargenomen.

- https://www.securecoding.com/blog/owasp-secure-coding-checklist/
- https://github.com/OWASP/CheatSheetSeries/tree/master/cheatsheets

De OSV-2020 U-module mist het gebruik van een vertrouwensketting (chain of trust) Een vertrouwensketting (chain of trust) zorgt ervoor dat alle ondertekende data verifieerbaar is. Gebruikers kunnen controleren dat de data digitaal ondertekend is door iemand die vertrouwd wordt door de hoogste autoriteit in de keten, in dit geval de Kiesraad zelf. Het ontbreken van digitale verificatie door middel van een vertrouwensketting, kan leiden tot manipulatie van de te verifiëren data, in dit geval de manipulatie van de stemdata en daarmee het verkiezingsproces. Het is daarom aan te raden gebruik te maken van een vertrouwensketting middels een zogenoemde Public Key Infrastructure (PKI). De volgende bron biedt algemene informatie met betrekking tot wat een PKI oplossing inhoudt:

- https://nl.wikipedia.org/wiki/Public_key_infrastructure

6 Risicocorrelatie

Op basis van de afzonderlijke bevindingen die tijdens dit onderzoek zijn gedaan, het mogelijk is om een aanvalspad te creëren. Let hierbij op dat er bij dit aanvalspad een ontbrekende stap is, waardoor het volledig pad momenteel enkel theoretisch blijft en praktisch nog niet uit te voeren is. Dit aanvalspad zit er als volgt uit:

Wanneer een aanvaller via social engineering een gemanipuleerd zip-bestand aan een legitieme gebruiker van de OSV-2020-U software levert, kan dit tot gevolg hebben dat de gebruiker het bestand importeert. Zelfs als de OSV-2020-U software het bestand niet verwerkt omdat het niet legitiem is, wordt het zip-bestand toch op de computer opgeslagen waar de software geïnstalleerd is. Dit betekent dat er ongewenste bestanden op het systeem kunnen achterblijven, zelfs als de beveiligingscontroles van de software het bestand niet als geldig herkennen.

Mocht de aanvaller nog de ontbrekende stap vinden om dit opgeslagen bestand ook via de OSV-2020-U software uit te laten voeren, dan kan dit resulteren in de uitvoer van code. Een mogelijk scenario kan zijn dat een aanvaller een HTML-document met kwaadaardige JavaScript-code gebruikt voor een Cross-Site-Scripting (XSS)-aanval. Als alternatief kan de aanvaller gebruik maken van een kwaadaardig uitvoerbaar bestand of een Java Server Pages (JSP) of XHTML-document met daarin kwaadaardige code. De aanvaller kan daarbij de bestaande Content-Security-Policy (CSP) HTTP response header omzeilen, waardoor de kwaadaardige code niet door deze defensieve maatregel wordt geblokkeerd.

Indien bovenstaand aanvalspad compleet wordt gemaakt, kan de uitvoer van eerdergenoemde code door de aanvaller misbruikt worden om de verkiezingsdata te manipuleren.

7 Bevindingsdefinities

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 opdrachtgever om afhankelijk van de specifieke verkiezingsprocessen en -omstandigheden het risiconiveau te bepalen. Fox-IT beschrijft daarnaast 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 echter de eindverantwoordelijkheid van de opdrachtgever om de kosten en baten van het overnemen van dit advies tegen elkaar af te wegen. 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 het verkiezingsproces of de applicatie in scope

Bij het inschatten van een risico worden er drie verschillende niveaus gehanteerd voor zowel de waarschijnlijkheid als impact namelijk, LAAG, GEMIDDELD en HOOG. Daarnaast kan het totale risico ook KRITIEK zijn. Volgens de formule “Risico = Waarschijnlijkheid x Impact” leidt dat tot het volgende schema:

	Lage impact	**Gemiddelde impact**	**Hoge impact**
Lage waarschijnlijkheid	LAAG	LAAG	GEMIDDELD
Gemiddelde waarschijnlijkheid	LAAG	GEMIDDELD	HOOG
Hoge waarschijnlijkheid	GEMIDDELD	HOOG	KRITIEK

8 Overzicht bevindingen

Bevinding	Omschrijving	Risico	Prioriteit
1	CSRF & CSP Bypass	Gemiddeld	Ja
2	Weak User Password Policy	Gemiddeld	Nee
3	Signature on Voting Data can not be Verified Using a Chain of Trust	Laag	Nee
4	Verification Check of the Import of the Election Definitions can be Improved	Laag	Nee
5	Log Contains Full Hash of the Verification Check of the Import of Election Candidate List	Laag	Nee
6	Enumeration of Blocked Accounts is Possible	Laag	Nee
7	Import of the Election Definitions can be Abused to Store any File Persistently	Laag	Nee

9 Technishe Bevindigen

Bevinding 1: CSRF & CSP Bypass

Risicoclassificatie	Gemiddeld		
Waarschijnlijkheid	Gemiddeld	**Gevolgen**	Gemiddeld

Betreft de systemen

- OSV-2020-U application, through the `primefaces.nonce` parameter

Omschrijving

The aforementioned asset is vulnerable to a Cross-Site Request Forgery[11] (CSRF) bypass by sending a malformed `primefaces.nonce` parameter in combination with a stateless viewstate parameter. In addition to this, due to the fact that the nonce is invalid, the HTTP Content-Security-Policy[12] (CSP) handler appears to be unable to apply the policy, resulting in no CSP header being sent. This can also be seen when investigating the server logs, where it is evident that something went wrong whilst applying the header:

```
14:15:24,543 WARN  [BEt4H7PQmvJT...-00002] [ElectCommonExceptionHandler] Fehler: messageKey=exceptio
n.unknown.message, [javax.faces.FacesException, Invalid CSP nonce, java.lang.IllegalArgumentExceptio
n, Illegal base64 character 27, Illegal base64 character 27]
```

Figure 1: Providing an invalid nonce value, containing an illegal character, results in the CSP handler beging unable to apply the policy

```
14:06:52,361 WARN  [udNb6NihZ88F...-<NO_USER>] [ElectCommonExceptionHandler] Fehler: messageKey=exce
ption.unknown.message, [javax.faces.FacesException, Invalid CSP nonce, java.lang.IllegalArgumentExce
ption, Input byte[] should at least have 2 bytes for base64 bytes, Input byte[] should at least have
 2 bytes for base64 bytes]
```

Figure 2: Providing an invalid, too short, nonce value results in the CSP handler beging unable to apply the policy

[11] CSRF tokens are unique, secret values that a web application assigns to each user's session to confirm that any submitted request is intentional and originates from the authenticated user, not an attacker. When a user performs an action on a web application, the CSRF token is submitted alongside the request. In this case, the `primefaces.nonce` value, which is normally used for the CSP header, also acts as a CSRF token.

[12] The `Content-Security-Policy` (CSP) header is a mechanism to control which (external) servers can host web resources, and how users' browsers are allowed to use them. The use of this HTTP header will result in protection against various attacks such as content injection (such as Cross Site Scripting (XSS) attacks), session hijacking attacks (the act of stealing another users' login session), and it protects users against clickjacking attacks (tricking users into clicking elements on external websites by hiding an `iframe` that covers the original button or element).

Risico

An attacker may leverage the lack of validation of CSRF tokens to (blindly) interact with the application and trigger unintended functionality. Additionally, the side-effect of a missing CSP header also means that all reflected cross site scripting, as well as click-jacking attacks become possible on affected web pages.

For example, an attacker could use the import function to upload an arbitrary file as shown in finding 7 op pagina 30. More specifically an attacker could upload a file, containing a HTML document with an XSS or a Java web shell, repeatedly without issue, due to the CSRF protection being bypassed. This is demonstrated in the screenshot below:

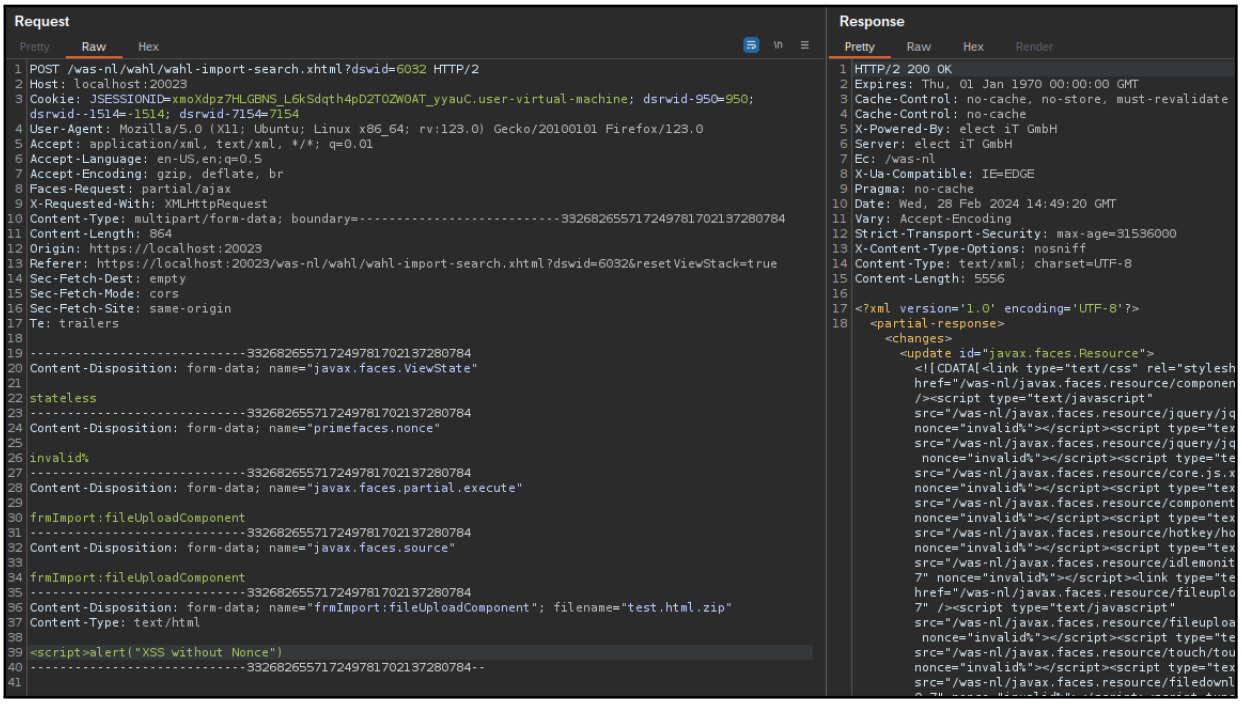

Figure 3: Upload Arbitrary HTML file containing XSS JavaScript code

Note that currently, due to time constraints, Fox-IT was unable to find a request to actually execute the uploaded file, but confirms that the upload is being accepted, since the uploaded file was found on disk:

```
[ 2024-02-28 15:52:47 ] user@user-virtual-machine:~/kiesraad2024/u-module/data/OSV2020-U/EP-HSB-20240606
$ cat ./data-storage/bestanden/-/import/importeren_verkiezing-20240228_155243096-1709126583526.zip
<script>alert("XSS without Nonce")</script>
```

Figure 4: File uploaded without nonce, was successfully stored on disk

This means that as soon as a request can be used to actually get the stored file executed, the impact would

be significantly increased, since this might result in either XSS or Remote Code Execution (RCE), especially because the CSP protection has been bypassed as well.

However, since this requires a chain of findings, because the secondary vulnerability that would execute the uploaded file is absent, the current impact has been reduced to “Medium”.

Aanbeveling

Before a request is dispatched to relevant handlers, verify that the `nonce` value is correct. In the event an invalid nonce value is sent, abort the request before any other business logic can be executed.

Furthermore, if the CSP header cannot be generated for some reason, either abort the request entirely, to prevent the output from being shown. Another option would be to return a similar header to that which is already in use, or send a very restrictive fallback header which prevents any form of content to load, as well as prevent any browsers from including the webpage.

For example, the following CSP could be sent in case of an error to block *any* form of interaction:

```
Content-Security-Policy: default-src 'none'; frame-ancestors 'none'
```

Bevinding 2: Weak User Password Policy

Risicoclassificatie	Gemiddeld		
Waarschijnlijkheid	Gemiddeld	**Gevolgen**	Gemiddeld

Betreft de systemen

- OSV-2020-U installation password policy
- OSV-2020-U application password policy

Omschrijving

Fox-IT has identified inconsistencies and weaknesses in the password policy of the OSV-2020-U application. The default password policy, and the policy during the installation of the OSV-2020-U software differ, which could lead to confusion.

Default password policy states that:

- The minimum password length is set to 9 characters;
- The use of special characters is required;

Password policy during installation states that:

- The minimum password length is set to 8 characters;
- The maximum password length is set to 20 characters;
- The use of special characters is required;

Lastly both the installation process and OSV-2020-U application itself do not screen user passwords against a list of known-bad passwords.

Risico

Attackers may try to guess passwords. If predictable passwords are used, then there is a higher chance that an attacker will manage to guess a password and thereby gain access to the respective account. After this, the attacker can use the account just as the normal user would.

Note however that a brute force mechanism is in place that blocks the account after 5 invalid attempt, and is only manually unblocked by admin intervention. This limits the likelihood of a successful attack, therefor the exploitability risk has been reduced from high to medium.

Aanbeveling

Based on the NIST[13] guidelines, Fox-IT created a set of recommendations to improve the password policy, and to stimulate correct use of strong passwords:

- Increase the minimum password length to 12, ideally as high as possible;
- Do not impose a maximum password length;
- Do not force users to include special characters in their passwords,[14] since this leads to more predictable and therefor weaker passwords;

[13] https://pages.nist.gov/800-63-3/.

[14] See "A.3 Complexity" in the NIST guidelines for more information: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

- Automatically screen user passwords against a list of known-bad passwords before they are allowed to be used.

Furthermore, if possible, use passphrases, as opposed to passwords as described above. Passphrases are passwords that consist out of an entire sentence. The use of passphrases, would allow the minimum password length requirement to be increased to a larger value such as 15 or even 20. This should result in passwords that are still easy for users to memorize and much harder to be cracked or guessed. Furthermore passphrases are less likely to end up in physical copies in the form of paper notes.

Lastly, make sure that password policies do not differ between different components of the software, such as the installation and usage of the OSV-2020-U application, make use of the same password policy to avoid confusion.

Bevinding 3: Signature on Voting Data can not be Verified Using a Chain of Trust

Risicoclassificatie	Laag		
Waarschijnlijkheid	Laag	**Gevolgen**	Gemiddeld

Betreft de systemen

- OSV-2020-U application

Omschrijving

The U-module software uses digital signatures to verify if the received voting data is valid. However, this works with separate (private/public) key pairs, which are uniquely associated with a location (and not with an individual), so that the files are not digitally signed when submitted. The digitally signed file is now sent to the receiving party, via the internet or on a USB stick. This setup does not contain a technical means to verify the authenticity of the public key itself, which effectively negates the intended authenticity of the signed data.

For more information regarding the import, transport and usage of the key material within the EP election setup, see:

- https://localhost:20023/was-nl/resources/help/TK/aanmaken-en-ophalen-public-key.htm
- https://localhost:20023/was-nl/resources/help/EP/aanmaken-private-key.htm
- https://localhost:20023/was-nl/resources/help/EP/inlezen-extern-aangemaakt-tell.htm

Risico

However, the setup contains public key material that is not digitally signed and therefore cannot be verified for authenticity. This allows an attacker to attempt to provide this public key themselves. Thus, an attacker could try to pose as a legitimate sender and thereby try to persuade the receiving party to enter this malicious key. Subsequently, the attacker could sign fraudulent voting data, effectively undermining the security measures as if the data were not digitally signed at all. Note that in practice, this can be quite difficult to exploit, which is why the probability of such an attack being carried out is considered low.

Note that after discussing this issue with the Kiesraad, they explained that verification of the counting data (“telbestanden”) is possible using the reports on paper. Furthermore, the paper trail is still the primary source of verification, which has also been ingrained into the Dutch law. Although, this means the software itself relies on an external process for verification, which requires a person to actually perform the check (there is no verification of this process in the software), the findings risk level has been reduced to “medium”, due to the fact that the physical paper process is the primary mandatory source of data for the election results.

Aanbeveling

Use digital signatures that can be verified using a chain of trust, for all files that are imported, to ensure their integrity and authenticity. Ensure that the accompanying certificate from the Certificate Authority (CA) is installed as the only one on all systems where this application runs, as well as in the browsers or certificate stores of users accessing the application.

In addition, each user should use a key (for example, through a hardware token) or certificate that can be traced back to a person. This ensures that any invalid voting data can be traced back to the individual responsible or, if they are unaware, to the system they used. This may help in finding the specific cause.

A possible implementation of this Public Key Infrastructure (PKI), could be carried out as follows:

- The installation file is digitally signed
- The Root CA is created and managed on a single system that does not have network access. The private key of this Root CA is located on this system.
- The Root CA certificate (and thus the associated public key) is stored in the Java keystore already in use and is provided by the aforementioned installation file.
- In addition to the installation file, a certificate file is provided containing the certificate and associated private key for each required user; this is person-specific, and each location will therefore receive a different file.
- The certificate file is loaded by the local administrator through the application, which stores it in the Java keystore.
- The application can then automatically sign voting data based on the logged-in user
- The voting data, along with the associated certificates, is exported for transport to the next location.
- The application can automatically verify the authenticity of the voting data because it has access to both the signed voting input and the corresponding certificates. In addition, the validity of these files can be validated because the same Root CA certificate is available everywhere.

More information regarding digital signatures and PKI can be found via the following URLs:

- https://nl.wikipedia.org/wiki/Digitale_handtekening
- https://nl.wikipedia.org/wiki/Public_key_infrastructure
- https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/vraag-en-antwoord/wat-is-een-elektronische-handtekening

Bevinding 4: Verification Check of the Import of the Election Definitions can be Improved

Risicoclassificatie	Laag		
Waarschijnlijkheid	Laag	**Gevolgen**	Gemiddeld

Betreft de systemen

- OSV-2020-U application, Election Definitions import

Omschrijving

Currently, the OSV-2020-U application requires an administrator to import election definition files and confirm their integrity. This done by simply selecting an option in a pull down-menu that indicates the hash code has been verified (this is the only option available in the pull down menu) as shown in the screenshot below:

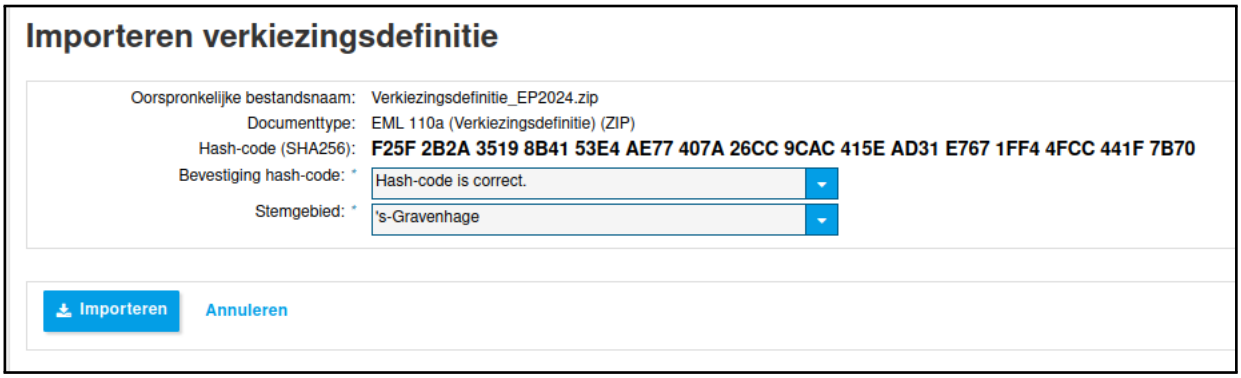

Figure 5: Current check of import of election definitions using a pull down menu selection

This approach relies heavily on the administrator's diligence and honesty, as there is no enforced mechanism to ensure that the hash code has been actively checked against a known good value.

Risico

If the verification of these definitions is not properly enforced, an attacker could manipulate the election definitions, without the OSV-2020-U administrator noticing that this was actually invalid, modified data. This could lead to incorrect ballot configurations. The current verification method does not provide sufficient assurance that the election definitions have not been tampered with.

Note that although in theory it might be possible to let an administrator import the modified election definitions using the OSV-2020-U application, it may cause problems at a later stage when processing voting data, due to the absence of the correct fields, which makes incorrect processing more noticeable. Due to this reason and the fact that administrator privileges are required, the exploitability has been reduced to a low risk and the impact has been reduced to a medium risk.

Aanbeveling

Modify the system to require administrators to manually input the full expected hash code during the import procedure.

Secondly, do not log the required valid hash in a place easy to access by the administrator, before the verification of the hash value has been validated, to prevent a blind copy-paste of the correct values.

Furthermore, it might be beneficial to publicly disclose the necessary hash value. This would allow citizens to follow the election process and independently confirm that the correct hash value has been entered (in addition to being able to verify the OSV-2020-U application source code).

Lastly, once the validation is done, always log both the required hash and given hash for auditing purposes.

Bevinding 5: Log Contains Full Hash of the Verification Check of the Import of Election Candidate List

Risicoclassificatie	Laag		
Waarschijnlijkheid	Laag	**Gevolgen**	Gemiddeld

Betreft de systemen

- OSV-2020-U application, through the election candidate list import functionality

Omschrijving

The system OSV-2020-U application is designed to request verification of part of the hash to ensure the integrity of the imported candidate list. However, it was discovered before the required hash value has been entered, the full hash value that is required is shown in the OSV-2020-U application log file, which is easily accessible by administrators as shown in the screenshot below:

```
16:14:02,639 INFO  [41JjUPP6A1Av...-00002] [EmlImportMapperHelper] EML: 230b, hashCode: D6C4 2094 7D
7C EB8F C489 804D F3BB E664 CFF1 7497 3C97 4349 E96E EB2E F1B7 BCC9
```

Figure 6: Import hash listed in the OSV-2020-U application log file

The primary purpose of hashing and verification is to detect any unauthorized alterations to the election candidate list. By logging the full hash value before the required hash value has been entered and making it visible to the administrator, the system undermines the verification process. An administrator could simply use the logged hash for verification, which negates the security benefits of hashing. As a result this practice could inadvertently facilitate a false sense of verification, as an administrator might be tempted to bypass the actual verification process by copying the hash directly from the log files instead of independently verifying it against a trusted source.

Risico

If the verification of these definitions is not properly enforced, an attacker could manipulate the election definitions, without the OSV-2020-U administrator noticing that this was actually invalid, modified data. This could lead to incorrect ballot configurations. The current verification method does not provide sufficient assurance that the election definitions have not been tampered with.

Note that although in theory it might be possible to get let an administrator import the modified election definitions using the OSV-2020-U application, it may cause problems at a later stage when processing voting data, due to the absence of the correct fields, which makes incorrect processing more noticeable. Due to this reason and the fact that administrator privileges are required, the exploitability has been reduced to a low risk and the impact has been reduced to a medium risk.

Aanbeveling

Revise the logging practices to exclude the full hash value from any location easily accessibly by the administrator, before the hash has been verified, including the OSV-2020-U application logs.

Furthermore, it might be beneficial to publicly disclose the necessary hash value. This would allow citizens to follow the election process and independently confirm that the correct hash value has been entered (in addition to being able to verify the OSV-2020-U application source code).

Lastly, once the validation is done, always log both the required hash and given hash for auditing purposes.

Bevinding 6: Enumeration of Blocked Accounts is Possible

Risicoclassificatie	Laag		
Waarschijnlijkheid	Laag	**Gevolgen**	Laag

Betreft de systemen

- OSV-2020-U application, through the user login found at `https://localhost:20023/was-nl/login.xhtml`

Omschrijving

The OSV-2020-U application user login mechanism can be tricked into revealing valid usernames, by disclosing the fact that a given account is blocked after 5 or more invalid attempts to log into the account. This is shown in the screenshot below:

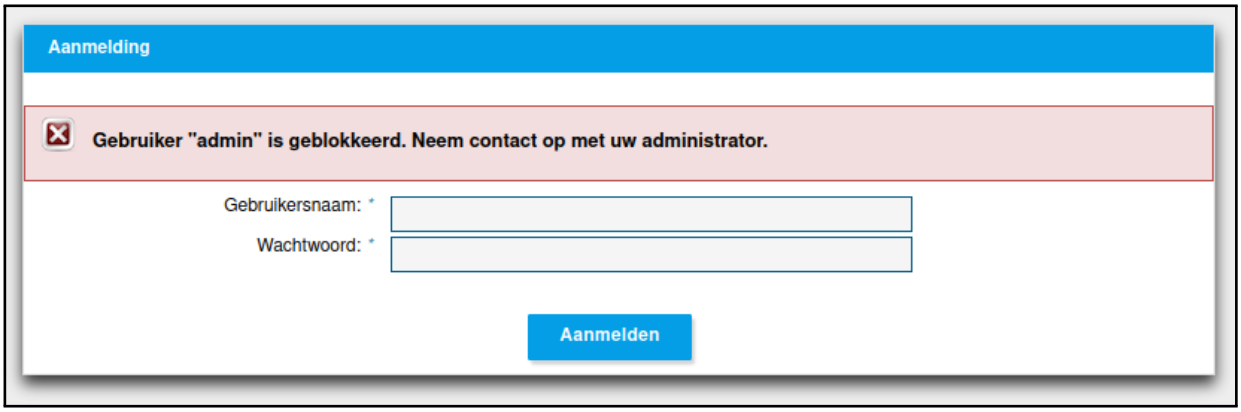

Figure 7: Account has been blocked message (after 5 failed attempts)

An attacker can exploit the aforementioned behavior by enumerating possible usernames, and attempting five passwords per username in order to intentionally cause the account to become locked, if it exists. If the account exists, a different response will be shown after which it can be determined that the account exists or not.

To increase the usefulness of the attack, an attacker can combine this with a password spraying attack, attempting six common passwords against a wide range of usernames. When the system blocks an account, the sixth password spray attempt will result into a message notifying the account has been blocked, which inadvertently confirms the existence of that account. This will lock all accounts that were found during the attack, and makes it thus more likely to result into an account which will also be unblocked within the available time the OSV-2020-U application is reachable.

Risico

An attacker can abuse the current user login mechanism, to obtain valid usernames which can then be used in a consecutive attack which aims to obtain the corresponding password.

Note, due to the short time the OSV-2020-U application is running, the fact that the account is blocked and a username by itself is not enough to login, both the exploitability risk and impact level have been reduced to “Low”.

Aanbeveling

The system should provide generic responses to failed login attempts that do not indicate whether the account is blocked, or even if the username exists. For example, the message “Your username or password is incorrect or the account is blocked”

If the aforementioned solution is not feasible, avoid blocking accounts alltogether, and use a rate limiting system that keeps increasing the lockout time after every attempt. For each invalid attempts a message such as “Invalid username or password” may be used, and any attempt past the rate limit could show a message such as “You’ve tried logging in too many times in a row. Please wait <time> before trying again.”

Bevinding 7: Import of the Election Definitions can be Abused to Store any File Persistently

Risicoclassificatie	Laag		
Waarschijnlijkheid	Laag	**Gevolgen**	Laag

Betreft de systemen

- OSV-2020-U application, through the election definitions import functionality

Omschrijving

The affected import module can be abused to upload arbitrary files, as long as the extension of the filename is altered to 'zip' in the applicable POST request as shown in the screenshot below:

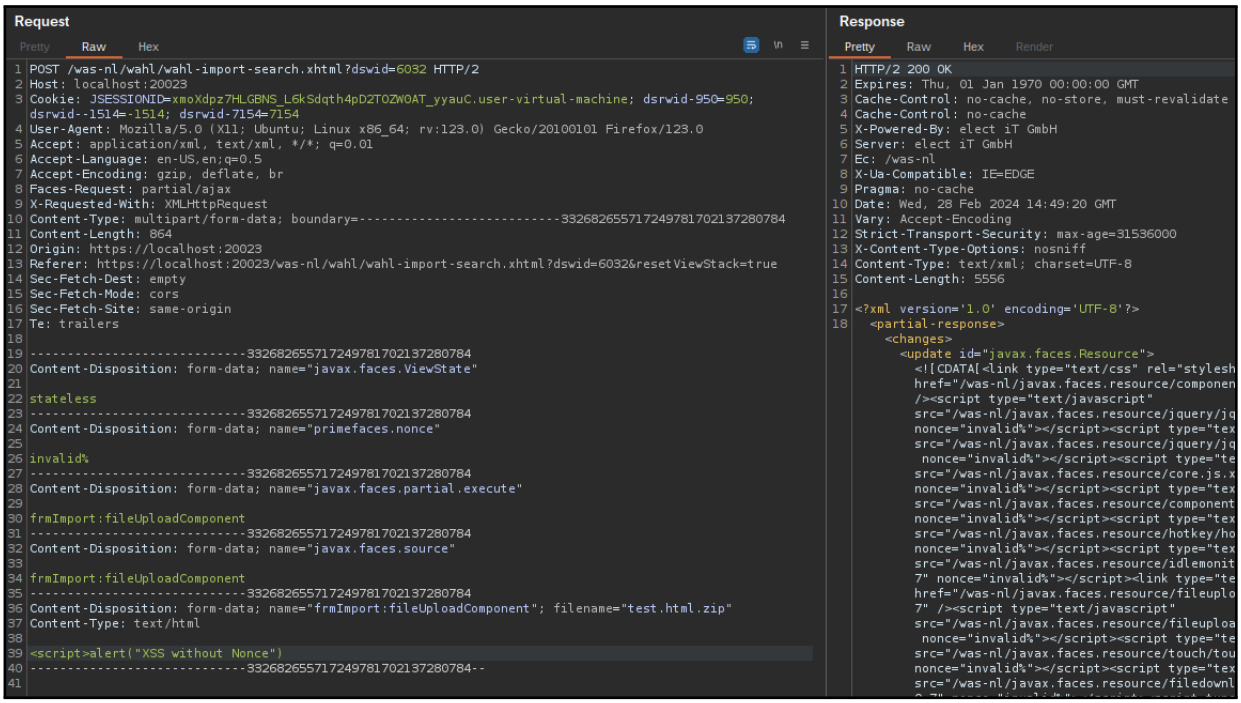

Figure 8: Upload Arbitrary HTML file containing XSS JavaScript code

Note that the file import validation does indeed not accept the invalid file, but stores any file given nonetheless. The only requirement is the 'zip' file extension, even though the file content can be something completely different. During the POST request, just altering the file extension is enough, the content type can be left as is. For example the "text/html" content type is accepted as well.

Risico

An attacker could use the import function to upload an arbitrary file, i.e. containing a HTML document containing malicious JavaScript code which may be used as part of a Cross-Site-Scripting (XSS) attack, a JSP or XHTML document containing a Java web shell or even a malicious executable.

Due to time constraints Fox-IT was unable to find a request to actually execute the uploaded file but confirms that the upload is being accepted and persistently stored, since the uploaded file was found on disk:

```
[ 2024-02-28 15:52:47 ] user@user-virtual-machine:~/kiesraad2024/u-module/data/OSV2020-U/EP-HSB-20240606
$ cat ./data-storage/bestanden/-/import/importeren_verkiezing-20240228_155243096-1709126583526.zip
<script>alert("XSS without Nonce")</script>
```

Figure 9: File uploaded without nonce, was successfully stored on disk

This means that as soon as a request can be used to actually open the stored file, the impact would be significantly increased, since this might result in either XSS or Remote Code Execution (RCE). The RCE would be either targeted at the PC running the OSV-2020-U application, via JSP or XHTML file containing a Java web shell or at any user connected to the running OSV-2020-U application (using a malicious executable or for example an excel file containing a `=cmd` formula). However, since this requires a chain of vulnerabilities, where the second vulnerability that executes the uploaded file has not been discovered yet, the current impact has been reduced to “Low”.

Lastly, due to the fact that the affected import functionality requires administrative privileges, the risk of overall exploitability has been reduced to “low” as well.

Aanbeveling

Ensure that the imported file contains valid data. If only invalid data is found, abort the request and return an error.

Alternatively, if disk storage is required during the validation process, make sure to remove this data from disk when the OSV-2020-U application determines that the given data is invalid.

Lastly make sure the file upload size is limited to a reasonable file size, to prevent filling up either memory or disk space.

Documentbeheer

Versiebeheer	
Referentie	PR-230511
Opdrachtgever	Kiesraad
Datum	March 22, 2024
Versie	1.0
Status	Definitief
Auteur(s)	

Deze versie vervangt alle voorgaande versies van dit document. Gelieve alle voorgaande exemplaren te vernietigen.

Distributielijst

Versie	Datum	Verspreidingsvorm	Naam
0.1	2024-03-01	PDF via Fox-IT ClientPortal	Kiesraad
0.3	2024-03-08	PDF via Fox-IT ClientPortal	Kiesraad
1.0	2024-03-22	PDF via Fox-IT ClientPortal	Kiesraad

Reviews

Versie	Datum	Gereviewd door	Functie
0.1	2024-03-07	Fox-IT	Technische QA
0.2	2024-03-08	Fox-IT	Grammatica QA
0.3	2024-03-14	De Kiesraad	QA
0.4	2024-03-20	Fox-IT	Executive QA

Wijzigingen

Versie	Datum	Naam	Opmerkingen
0.1	2024-03-01	Fox-IT	Voorlopige versie
0.2	2024-03-07	Fox-IT	Review voorlopige versie verwerkt en all hoofdstukken benodigde voor de finale versie toegevoegd

Versie	Datum	Naam	Opmerkingen
0.3	2024-03-08	Fox-IT	Interne review verwerkt
0.4	2024-03-15	Fox-IT	Review van de Kiesraad verwerkt
0.5	2024-03-21	Fox-IT	Interne review verwerkt
1.0	2024-03-22	Fox-IT	Uiteindelijke versie

Gerelateerde Documenten

Versie	Datum	Omschrijving	Opmerkingen
1.1	2024-02-08	OSV-2020 Software Penetratietest KS & PP modules voor de Europese verkiezingen	Penetratietest-rapport

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.

CLASSIFICATIE
OPENBAAR

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