Kiesraad

Resultaten Penetratietest OSV2020-U

Definitief
Referentie: 2022-0669
2 december 2022

pwc

Inhoudsopgave

1 Managementsamenvatting 3

1.1 Resultaat onderzoek 3

1.2 Belangrijkste aanbevelingen 5

2 Details van ons onderzoek 6

3 Detailbevindingen 8

3.1 De client-side air-gap wordt niet geforceerd waardoor gebruikers de applicatie kunnen gebruiken terwijl zij verbonden zijn met het internet 8

3.2 Een gebrek aan hardening van de systemen maakt verschillende aanvalspaden mogelijk 11

3.3 Een beheerder kan zijn eigen wachtwoord wijzigen zonder dat daar het huidige wachtwoord voor nodig is 13

3.4 Waarschuwingen over de aantallen en totalen van de getelde stemmen kunnen worden genegeerd waardoor mogelijk foutieve steminvoer kan worden geaccepteerd 15

3.5 Een MySQL database gebruikt voor OSV2020-U wordt na verwijderen van de applicatie niet geleegd of verwijderd 17

3.6 Het is mogelijk om een sessiecookie in meerdere sessies tegelijkertijd te gebruiken 18

3.7 De OSV2020-U applicatie maakt gebruik van enkele verouderde en kwetsbare softwarecomponenten 20

3.8 Directe aanpassingen in de database kunnen leiden tot inconsistenties tussen data die gebruikers zien in de front-end 22

3.9 Onnodige functionaliteit en data binnen de applicatie en database vergroten het aanvalsoppervlak van de applicatie 24

A. Toelichting classificaties 26

A.1. Risico classificatie 26

A.1.1. Kans 26

A.1.2. Impact 26

A.2. Inspanning classificatie 27

A.2.1. Kosten 27

A.2.2. Tijdsinvestering 27

B. Disclaimer 28

PricewaterhouseCoopers Advisory N.V., Thomas R. Malthusstraat 5, 1066 JR Amsterdam, Postbus 9616, 1006 GC Amsterdam
T: 088 792 00 20, F: 088 792 96 40, www.pwc.nl

1 Managementsamenvatting

PricewaterhouseCoopers Advisory N.V. (hierna: PwC) heeft in opdracht van De Kiesraad in de periode van 3 oktober 2022 tot en met 14 oktober 2022 een penetratietest uitgevoerd op Ondersteunende Software Verkiezingen module Uitslagvaststelling (OSV2020-U). Wij rapporteren in dit rapport dan ook naar de stand van OSV2020-U op 14 oktober 2022.

De doelstelling van deze opdracht was het beantwoorden van de volgende vragen op basis van een penetratietest:

- Welke kwetsbaarheden en risico's op het gebied van informatiebeveiliging zijn te onderkennen in het testobject?
- Welke maatregelen kunnen worden getroffen om de geconstateerde risico's te mitigeren?

Het eerste hoofdstuk presenteert een managementsamenvatting van onze bevindingen. Het tweede hoofdstuk schetst de context en de reikwijdte van deze opdracht. Het derde en laatste hoofdstuk zet onze bevindingen in detail uiteen op basis van de uitgevoerde werkzaamheden. Deze gedetailleerde bevindingen bevatten een risicoclassificatie en een inschatting van de inspanning die nodig is om het geïdentificeerde risico te mitigeren. Een toelichting op de risico- en oplossingsclassificatie is opgenomen in Appendix A.

1.1 Resultaat onderzoek

Uit ons onderzoek naar de beveiliging rondom de OSV2020-U software zijn negen (9) bevindingen voortgekomen.

Een belangrijke factor bij het bepalen van het restrisico[1] van deze bevindingen is de aanname dat de omgeving wordt opgezet volgens de door De Kiesraad meegeleverde installatiehandleiding en conform de hierin beschreven maatregelen.

Wij hebben geen bevindingen met restrisico hoog geïdentificeerd. Eén (1) bevinding heeft als restrisico midden, namelijk het niet technisch afdwingen door OSV2020-U van de client-side air-gap[2]. De overige acht (8) bevindingen hebben restrisico laag. De totstandkoming van de restrisico's heeft als voorwaarde dat de software wordt geïnstalleerd op een systeem in een afgesloten ruimte. Daarnaast dienen de server en de systemen, gebruikt om de OSV2020-U applicatie te benaderen, niet verbonden te zijn met het internet en dat de applicatie vereist dat stemaantallen altijd door twee verschillende gebruikers worden ingevoerd. Tot slot heeft de Kiesraad aangegeven dat er een protocol aanwezig is voor de controle van de stemaantallen in OSV2020-U en dat de papieren stemmen en stemaantallen altijd leidend zijn. Deze maatregelen spelen een belangrijke mitigerende rol en verlagen daarmee het bruto risico van de onderstaande bevindingen naar het genoemde restrisico. Indien niet wordt voldaan aan de installatievoorschriften uit de handleiding en de naleving van het eerder genoemde protocol ter controle van de stemaantallen is de risicoclassificatie van onderstaande bevindingen hoger, namelijk het genoemde bruto risico en kunnen zich mogelijke andere kwetsbaarheden voordoen.

In Tabel 1 is een overzicht weergegeven van de geïdentificeerde bevindingen. In de paragrafen hieronder volgt een korte samenvatting van deze bevindingen en de daaraan verbonden impact op de veiligheid van de OSV2020-U applicatie.

Uit bevindingen 3.1, 3.2 en 3.9 volgt dat het aanvalsoppervlak van de applicatie en de omgeving waarin deze wordt opgezet verkleind kan worden. Momenteel zijn er verschillende mogelijke

[1] Wij maken in ons rapport onderscheid in een classificatie naar bruto risico en restrisico. Het bruto risico is het risico als de compenserende maatregelen zoals benoemd in de installatiehandleiding of de maatregelen in het protocol ter controle van de stemaantallen niet of deels zijn getroffen. Het restrisico is het risico wat overblijft indien alle compenserende maatregelen zoals benoemd in de installatiehandleiding en de maatregelen in het protocol ter controle van de stemaantallen effectief zijn ingericht.

[2] Met air-gap wordt bedoeld dat een systeem niet in verbinding staat met het internet. Client-side slaat op de systemen die door gebruikers worden gebruikt om de applicatie te benaderen.

aanvalspaden waarmee een aanvaller of kwaadwillende medewerker mogelijk foutieve stemaantallen in OSV2020-U kan plaatsen of een account van een gebruiker op dezelfde werkplek kan overnemen (3.2). Ook wordt momenteel niet afgedwongen dat een gebruiker van OSV2020-U niet verbonden is met het internet. De implementatie van deze zogeheten client-side air-gap is daarnaast eenvoudig te omzeilen (3.1). Tot slot bevat de software onnodige componenten en functionaliteit die een aanvaller mogelijk zouden kunnen helpen bij het uitvoeren van een aanval (3.9).

De OSV2020-U server- en webapplicaties bevatten daarnaast verschillende kwetsbaarheden die onder bepaalde omstandigheden kunnen leiden tot het overnemen van een (beheer)account of het mogelijk beperken van de beschikbaarheid van de applicatie, zo blijkt uit bevindingen 3.3, 3.6 en 3.7. Een gebruiker met de rol beheerder kan momenteel zijn eigen wachtwoord wijzigen zonder dat daar het huidige wachtwoord voor nodig is. Een aanvaller met kortstondige toegang tot een dergelijk account kan deze daardoor overnemen door het wachtwoord te veranderen (3.3). Daarnaast is het mogelijk om gelijktijdig op twee plekken als één gebruiker ingelogd te zijn. Hoewel dit niet lukt door twee keer in te loggen, kan een sessiecookie, een unieke waarde gebonden aan de sessie van de gebruiker, wel handmatig gekopieerd en toegevoegd worden op een andere werkplek. Een aanvaller moet daarvoor wel eerst een sessiecookie bemachtigen, maar krijgt daarmee wel toegang tot de sessie van de gebruiker (3.6). Verder worden enkele verouderde en kwetsbare softwarecomponenten gebruikt. Hoewel het tijdens het onderzoek niet gelukt is de kwetsbaarheden in deze componenten te misbruiken, kan succesvol misbruik van deze kwetsbaarheden leiden tot impact op de beschikbaarheid van de applicatie en vertrouwelijkheid van de data in database (3.7).

Bevinding 3.4 toont aan dat het mogelijk is stemaantallen te accepteren die niet voldoen aan de vooraf opgestelde richtlijnen en logische checks. Dit kan ertoe leiden dat er, per ongeluk of met opzet, niet-realistische aantallen stemmen in OSV2020-U worden doorgevoerd (3.4). Bevinding 3.8 laat daarnaast zien dat het mogelijk is dat verschillende gebruikers van OSV2020-U andere stemaantallen te zien kunnen krijgen indien een beheerder handmatig aanpassingen heeft gedaan in de database. Hoewel hiervoor een beheeraccount en toegang tot server waar de OSV2020-U database op staat nodig is, kan een dergelijke situatie in uitzonderlijke gevallen wel leiden tot verkeerde stemaantallen in OSV2020-U (3.8).

Tot slot zijn er zoals beschreven in bevinding 3.5 verbeteringen mogelijk in het proces rond het deinstalleren en verwijderen van de applicatie. Als OSV2020-U gebruikt wordt met een losstaande database, dan wordt deze database niet geleegd of verwijderd na het deinstalleren en verwijderen van de OSV2020-U applicatie. Hierdoor kan onbedoeld OSV2020-U data achterblijven (3.5).

Tabel 1 - Overzicht bevindingen

#	Bevinding	Bruto risico	Restrisico	Inspanning
3.1	De client-side air-gap wordt niet geforceerd waardoor gebruikers de applicatie kunnen gebruiken terwijl zij verbonden zijn met het internet	Midden	Midden	Midden
3.2	Een gebrek aan hardening van de systemen maakt verschillende aanvalspaden mogelijk	Midden	Laag	Midden
3.3	Een beheerder kan zijn eigen wachtwoord wijzigen zonder dat daar het huidige wachtwoord voor nodig is	Midden	Laag	Laag
3.4	Waarschuwingen over de aantallen en totalen van de getelde stemmen kunnen	Midden	Laag	Laag

#	Bevinding	Bruto risico	Restrisico	Inspanning
	worden genegeerd waardoor mogelijk foutieve steminvoer kan worden geaccepteerd			
3.5	Een MySQL database gebruikt voor OSV2020-U wordt na verwijderen van de applicatie niet geleegd of verwijderd	○ Laag	○ Laag	○ Laag
3.6	Het is mogelijk om een sessiecookie in meerdere sessies tegelijkertijd te gebruiken	○ Laag	○ Laag	○ Laag
3.7	De OSV2020-U applicatie maakt gebruik van enkele verouderde en kwetsbare softwarecomponenten	○ Laag	○ Laag	○ Laag
3.8	Directe aanpassingen in de database kunnen leiden tot inconsistenties tussen data die gebruikers zien in de front-end	○ Laag	○ Laag	○ Laag
3.9	Onnodige functionaliteit en data binnen de applicatie en database vergroten het aanvalsoppervlak van de applicatie	○ Laag	○ Laag	○ Midden

1.2 Belangrijkste aanbevelingen

De aanbevelingen in deze rapportage kunnen worden doorgevoerd zonder dat dit de aanschaf van nieuwe hard- of software vereist. Wij verwachten dat alle bevindingen met beperkte inspanning verholpen kunnen worden. Wij raden aan om, in eventueel nauw overleg met de leverancier van de software, de volgende aanpassingen door te voeren:

- Pas hardening toe op de systemen waarop OSV2020-U wordt geïnstalleerd en gebruikt, zoals het beperken van de mogelijkheden voor gebruikers om de configuratie te wijzigen en het beperken van functionaliteit en meegeleverde software(componenten) tot wat noodzakelijk is voor het doel van OSV2020-U.
- Voorkom dat gebruikers hun wachtwoord kunnen wijzigen zonder dat daarvoor het huidige wachtwoord nodig is.
- Verander de client-side air-gap waarschuwing in een blokkade en overweeg een implementatie die minder makkelijk te omzeilen is.
- Voorkom dat waarschuwingen over niet-realistische of onlogische stemaantallen genegeerd kunnen worden.
- Verwijder of leeg de gebruikte database bij de-installatie indien OSV2020-U met een losstaande database wordt gebruikt, of waarschuw de gebruiker dat de data met een de-installatie niet verwijderd wordt.
- Bind sessiecookies aan IP-adressen zodat een sessiecookie niet op twee apparaten tegelijkertijd gebruikt kan worden.
- Update verouderde en kwetsbare software naar de meest recente, stabiele versie.
- Ga na of de gebruikte caching software ook in reguliere situaties inconsistenties kan veroorzaken in de front-end.

Tenslotte adviseren wij, voor zover dat mogelijk is, toe te zien op de naleving van de installatievoorschriften voor OSV en het controleprotocol voor de stemaantallen.

2 Details van ons onderzoek

In de periode van 3 oktober 2022 tot en met 14 oktober 2022 hebben wij een penetratietest uitgevoerd op OSV2020-U. OSV202 is een applicatie die gebruikt wordt ter ondersteuning van het verkiezingsproces, bestaande uit drie modules. Het onderwerp van de penetratietest was de module voor uitslagvaststelling (U). OSV2020-U wordt gebruikt bij het vaststellen van de verkiezingsuitslag en het bepalen van de zetelverdeling door gemeentelijke stembureaus, hoofdstembureaus en centrale stembureaus. De overige twee modules van OSV202 vielen buiten de scope van deze penetratietest.

De doelstelling van deze opdracht was het beantwoorden van de volgende vragen door middel van een penetratietest:

- Welke kwetsbaarheden en risico's op het gebied van informatiebeveiliging zijn te onderkennen in het testobject?
- Welke maatregelen kunnen worden getroffen om de geconstateerde risico's te mitigeren?

Reikwijdte

Het object van onderzoek betreft het stelsel van beveiligingsmaatregelen rondom OSV2020-U, zoals door u aan ons aangeleverd en geïnstalleerd op onze eigen infrastructuur.

Testen vanuit het ongeautoriseerde (blackbox) als het geautoriseerde (greybox) perspectief vallen beiden binnen de scope van de opdracht.

- De blackbox-test heeft een brede scope: dit wil zeggen, onze tooling scant op een breed scala aan kwetsbaarheden.
- De tooling die in de blackbox-test wordt gebruikt, wordt ook in de greybox-test gebruikt. De greybox-test betreft een test vanuit het geautoriseerde perspectief.

Buiten scope vallen:

- Het uitvoeren van een code review (whitebox-test).
- Het vaststellen of de door u aangeleverde software de juiste software is (known good).

Wij hebben onderstaande richtlijnen als leidraad voor de penetratietest gehanteerd:

- De OWASP Application Security Verification Standard (ASVS) (Level 1).
- De OWASP Top 10.
- De SANS Top 25.
- NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS).
- NCSC ICT-beveiligingsrichtlijnen voor webapplicaties.

Wij hebben onze werkzaamheden gebaseerd op de door de Kiesraad verstrekt software en instructies. De Kiesraad heeft ten behoeve van het onderzoek de OSV2020-U software en bijbehorende documentatie aangeleverd. Tabel 2 geeft een overzicht van de aangeleverde bestanden.

Tabel 2 - Overzicht van de door de Kiesraad aangeleverde bestanden

Bestandsnaam (SHA-256 hash)
Bijlage 3 Systeemvereisten OSV2020-U (uitslagvaststellingsoftware).pdf (2360ce7cece6b7f4b4a4ebcb87fcf0a12b654187e83862f587dd8975999f257b)

Bestandsnaam (SHA-256 hash)
Hashcode Amsterdam.txt (b6612d765ed1678f4f2307ffdb783026aeac6c434364d72f3261360b0dce0c76)
Hashcode Kieskring NH.txt (0dbb26c5777e9140e9d8f72c4d0f6b54cf587084a7e0acb3f0d865887e554c30)
Kandidatenlijsten_PS2023_NoordHolland_Amsterdam.eml.xml (d8e879b429fc09584207db4eafb2f3c9b8acbaeafefa225c95cc0f6b45f57c79)
nl-installer-was-1.8.0-OSV2020-U-installer.zip (8fe3f85a84fb823605f08aed4ecbb2e521f589f8a6c2e66e8b1b94940b0dfd1f)
nl-installer-was-1.8.0-OSV2020-U-installer.zip.sha256 (952f13ee8a8b432e46e7959cf6ba0f2fef16d4ee3e65fa1c27af1ac83b9b7ed0)
nl-installer-was-1.8.0-OSV2020-U-installer.zip.sha512 (f4fed8aa1c99ab568f9b859f1f147d6a90e22144495f8a450a220c2b299ff650)
Totaallijsten_PS2023_NoordHolland.eml.xml (3bad5119b3a1cb0c589dd70778d25f5e83ddb55e61b59306566eef818ee8ebb9)
U+hostname+en+certificaat+toevoegen-OSV2020-U-GR+2022.pdf (753eac9fe52b159f96ad6a4dabe1f7126cb13a381d0b18e10d948612b8937227)
U+Stappenplan+OSV2020-U-GR+2022.pdf (c606ce375825f509789a947d41b58c5091220584ae26d58d026edb48e8bfbdc6)
Vaststellen_van_de_authenticiteit-van_de_OSV2020_software_20210910.pdf (aacacb66c39ab67564b20d91df04be160956cd3df8702ab15aa2902098f27760)
Verkiezingsdefinitie_PS2023_NoordHolland_TEST.eml.xml (f065dd86e31a97c4689dd39496a7ca48d7b48b1cd86f06a6bee22afa73211e97)
Voorwaarden_voor_gebruik_OSV2020-U_20211019 (2).pdf (fba1bd6a006a2fdeb0a3d1b55a10091a626212224be7c5615414d9d5ee112959)

Voor het onderzoek is gebruikgemaakt van de aangeleverde versie van OSV2020-U. Het bestand `nl-installer-was-1.8.0-OSV2020-U-installer.zip` bevat installatiebestanden voor Linux, OSX en Windows. De software is ten behoeve van de penetratietest zowel op Windows als op Linux geïnstalleerd. Op verzoek van de Kiesraad heeft het onderzoek zich voornamelijk gericht op de versie voor Windows. De softwareversie na installatie met de aangeleverde installatiebestanden is versie 1.8.0 – 202209231358.

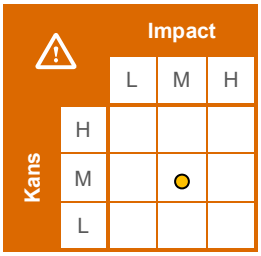
De details van alle bevindingen en de daarbij horende aanbevelingen hebben wij opgenomen in de volgende paragrafen. Per bevinding zijn daarnaast indien van toepassing de CVSS 3.1 score en string[3] vermeld, en de relevante ASVS 4.0.3 richtlijn[4].

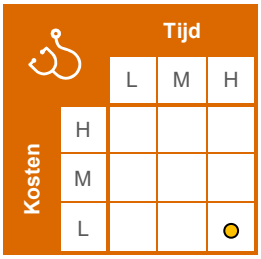
[3] https://www.first.org/cvss/v3.1/specification-document
[4] https://owasp.org/www-project-application-security-verification-standard/

3 Detailbevindingen

In de onderstaande secties worden onze bevindingen in detail omschreven. Per bevinding wordt een beschrijving gegeven van de bevinding, waar de bevinding binnen de software is aangetroffen, een risicoclassificatie en een voorgestelde oplossing. Een toelichting op de classificaties is te vinden in bijlage A. Met een grijs bolletje in de matrix voor risicoclassificatie geven wij het bruto risico aan mocht deze verschillen van het restrisico.

3.1 De client-side air-gap wordt niet geforceerd waardoor gebruikers de applicatie kunnen gebruiken terwijl zij verbonden zijn met het internet

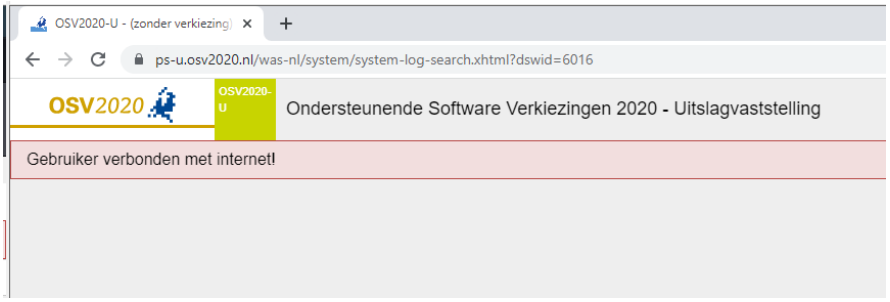




CVSS score	CVSS vector string
N/A	N/A
ASVS categorie en richtlijn	
N/A	

Bevinding

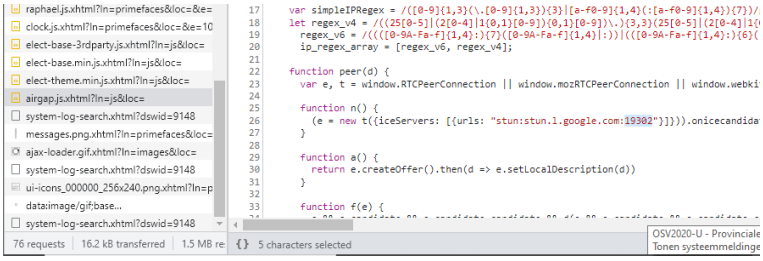
De applicatie maakt gebruik van JavaScript om te controleren of een gebruiker van de applicatie verbonden is met het internet. Echter, momenteel levert deze check alleen een melding op in de interface van de gebruiker en in het meldingenoverzicht van de beheerder. De applicatie kan verder als normaal gebruikt worden. Figuur 1 laat de melding zien zoals een gebruiker deze te zien krijgt bij gebruik van de applicatie en een verbinding met het internet.



Figuur 1 - Melding over verbinding met het internet

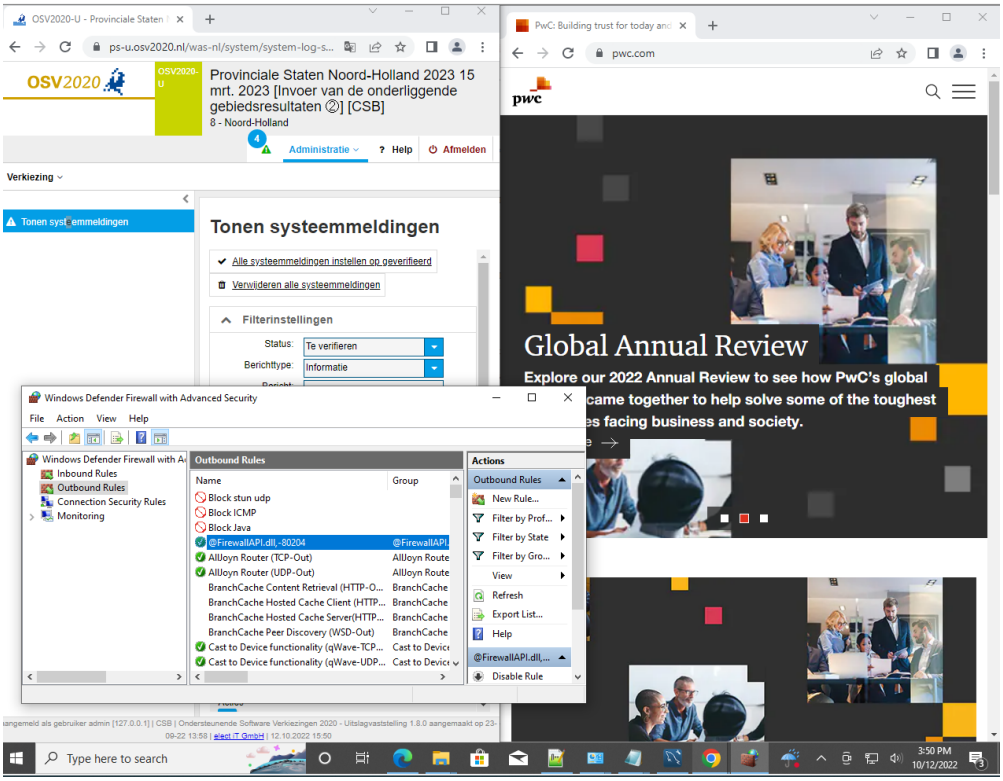
Als de applicatie benaderd kan worden via een systeem dat ook toegang heeft tot of bereikbaar is via het publieke internet biedt dit verschillende kansen voor een aanvaller. Een kwaadwillende medewerker zou op deze manier eenvoudig stemaantallen kunnen doorsturen naar een externe partij. Anderzijds biedt het voor een mogelijke externe aanvaller ook een manier om de applicatie(server) te bereiken en zo een verdere aanval op te zetten.

Daarnaast is de huidige implementatie van deze client-side air-gap eenvoudig te omzeilen. De huidige implementatie gebruikt een STUN request naar een server, zoals weergegeven in Figuur 2. Indien succesvol, wordt uit dit request het IP-adres gehaald vanaf waar dit request afkomstig is. Als dit een extern IP-adres is wordt geconcludeerd dat er verbinding is met het internet en wordt de waarschuwing weergegeven.



Figuur 2 - Fragment van de implementatie van de client-side air-gap

Deze methode maakt echter gebruik van één specifieke UDP port. Door uitgaand verkeer naar deze port te blokkeren wordt de air-gap omzeild en wordt er bij zowel de gebruiker als beheerder geen melding weergegeven. Figuur 3 laat zien dat door het toevoegen van een firewall regel die dit verkeer blokkeert, internettoegang mogelijk is terwijl OSV2020-U gebruikt wordt en geen melding wordt weergegeven.



Figuur 3 - Het omzeilen van de client-side air-gap

Object(en)

Deze bevinding heeft betrekking op de gebruikerskant en webinterface van de OSV2020-U applicatie.

Risicoclassificatie

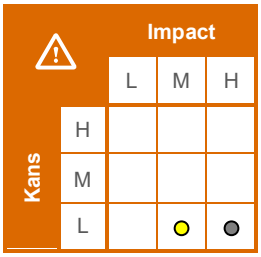
Een kwaadwillende gebruiker kan eenvoudig de air-gap omzeilen zonder dat een beheerder dit door heeft. Het hebben van een externe verbinding vergroot het aanvalsoppervlak van de omgeving. Een aanvaller met toegang over het internet tot één werkplek kan deze gebruiken om verdere aanvallen op te zetten naar andere gebruikers en de server waar OSV2020-U op draait. Daarnaast is het mogelijk gegevens uit OSV2020-U direct via het internet door te sturen naar een externe partij. Hoewel informatie zoals aantallen stemmen later openbaar zullen worden, kan dit er wel toe leiden dat deze informatie vroegtijdig lekt. Wij classificeren de mogelijke impact daarom als midden.

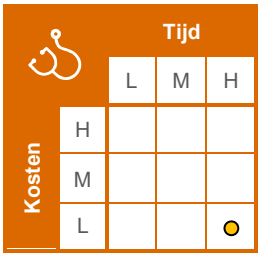
Wij classificeren de kans op misbruik als midden. Een gebruik kan door de broncode van de OSV2020-U front-end te bekijken eenvoudig zien hoe de controle op de air-gap werkt. Het omzeilen is daarnaast eenvoudig, een gebruiker hoeft enkel een regel in de lokale firewall toe te voegen.

Voorgestelde oplossing

Wij raden aan de air-gap aan de client-side te forceren in plaats van enkel een waarschuwing te tonen. Aanvullend kan er gekeken worden naar een andere implementatie van de client-side air-gap. Momenteel wordt er gebruikgemaakt gemaakt van JavaScript om enkele checks uit te voeren, de mogelijkheden voor het afdwingen van controleren of er een netwerkverbinding is zijn hiermee beperkt. Voor een andere benadering zou bijvoorbeeld gebruikgemaakt kunnen worden van een lokale security policy op de systemen van eindgebruikers, waarmee voorkomen wordt dat zij netwerkinstellingen kunnen aanpassen. Tot slot zou gebruikgemaakt kunnen worden van centraal beheerde systemen voor gebruikers, waardoor een beheerder meer mogelijkheden krijgt voor het afdwingen van de air-gap.

3.2 Een gebrek aan hardening van de systemen maakt verschillende aanvalspaden mogelijk





CVSS score	CVSS vector string
3.6 (Laag)	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:L
ASVS categorie en richtlijn	
V1: Architecture, Design and Threat Modeling Requirements, 1.9.1	

Bevinding

Naast de systeemeisen en implementatie van de air-gap worden er in de installatievoorschriften geen eisen gesteld aan de systemen waarop OSV2020-U wordt geïnstalleerd. Dit kan ertoe leiden dat er voor kwaadwillende gebruikers en beheerders, of aanvallers met toegang tot een van de systemen die gebruikt worden voor OSV2020-U, meerdere mogelijke aanvalspaden ontstaan.

Een voorbeeld hiervan is het verkrijgen van een man-in-the-middle positie tussen een gebruiker en de server waarop OSV2020-U draait. Een aanvaller met toegang tot een van de systemen voor eindgebruikers kan op een dergelijk systeem een proxy instellen en het verkeer omleiden via zijn eigen systeem. Hierdoor kan hij verkeer dat de legitieme gebruiker verstuurt, zoals bijvoorbeeld aantallen stemmen, inzien en aanpassen. Hoewel het risico beperkt is door de leidende rol van de papieren stemmen, kan op deze manier wel een verkeerd aantal stemmen in OSV2020-U terechtkomen.

Daarnaast worden gegevens zoals aantallen stemmen of namen van kandidaten onversleuteld opgeslagen. Een beheerder met toegang tot de database kan deze daardoor eenvoudig direct aanpassen.

Tot slot maken eindgebruikers vaak gebruik van gedeelde systemen om in te loggen op OSV2020-U. Deze gebruikers benaderen OSV2020-U met een browser. Bij het inloggen stelt de browser voor om de inloggegevens van de gebruiker op te slaan. Het is hierdoor mogelijk dat gebruikers die hiervoor kiezen (per ongeluk) hun account toegankelijk maken voor andere gebruikers.

Object(en)

Deze bevinding is van toepassing op de systemen waarop OSV2020-U gehost en gebruikt wordt.

Risicoclassificatie

Wij classificeren de impact als midden. Een aanvaller of kwaadwillende gebruiker die een man-in-the-middle positie of toegang tot de database weet te verkrijgen kan een grote impact hebben op de beschikbaarheid en integriteit van de OSV2020-U applicatie en de data. Het is hierdoor mogelijk dat een aanvaller invloed heeft op bijvoorbeeld de stemaantallen in de database. De Kiesraad heeft echter aangegeven dat er een protocol aanwezig is om de aantallen in OSV te verifiëren en dat de papieren stemmen en stemaantallen altijd leidend zijn, waardoor de impact in de context van het verkiezingsproces beperkt is tot bijvoorbeeld (tijdelijk) een verkeerd aantal stemmen of een verkeerde zetelverdeling in OSV2020-U. Dit zal niet direct leiden tot verkeerde definitieve uitslagen maar wel tot aanzienlijke reputatieschade.

Wij classificeren de kans op misbruik als laag. Om een man-in-the-middle positie te verkrijgen heeft een aanvaller toegang nodig tot een systeem van een gebruiker en het netwerk waarover gebruikers verbinden met de OSV2020-U applicatie. Hoewel de stemdata in de database eenvoudig te vinden en aan te passen is omdat deze onversleuteld is, is voor toegang tot de database is wel een account van een beheerder nodig.

De kans voor het (per ongeluk) opslaan van een wachtwoord in de browser schatten wij hoger in. Gebruikers kunnen uit gewoonte ervoor kiezen een wachtwoord op te slaan of zich niet bewust zijn dat ze hiermee mogelijk andere toegang geven tot hun account.

Voorgestelde oplossing

Wij adviseren om hardeningsmaatregelen toe te passen op de omgeving en systemen die gebruikt worden voor OSV2020-U om zo het aanvalsoppervlak te verkleinen. Om een man-in-the-middle aanval te voorkomen kan bijvoorbeeld gebruik gemaakt worden van client certificaten. Dit zijn certificaten die uitgegeven worden aan gebruikers waarmee zij vervolgens zichzelf kunnen authentiseren richting de server. Indien een aanvaller dan een man-in-the-middle positie heeft verkregen weigert de server een verbinding met de client op te zetten.

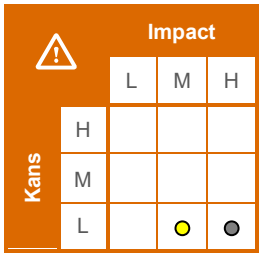
Een andere maatregel is het beperken van de mogelijkheden die gebruikers hebben tot het wijzigen van de configuratie op de clientsystemen. Zo kan bijvoorbeeld het wijzigen van de proxyinstellingen op Windows beperkt worden door middel van een Group Policy Object (GPO) of via een Local Group Policy[5]. Hiervoor kan gebruik gemaakt worden van een centraal beheerde Active Directory omgeving, of kan op gebruikte systemen handmatig een policy toegevoegd worden die het bewerken van de netwerkinstellingen beperkt. Hiervoor is aanvullende software en/of hardware nodig en maakt het opzetten van de OSV2020-U omgeving waarschijnlijk complexer.

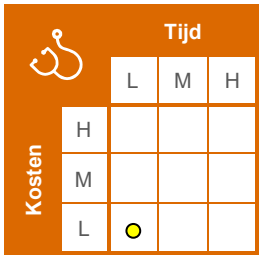
Daarnaast kan voor het opslaan van gevoelige waarden zoals de stemaantallen gebruik worden gemaakt van versleuteling. Hierdoor wordt het voor een beheerder of aanvaller met directe toegang tot de database lastig om direct waarden zoals stemaantallen aan te passen. Voor het opslaan van een sleutel voor de gebruikte versleuteling kan bijvoorbeeld gebruikgemaakt worden van de al aanwezige keystore.

Het opslaan van het wachtwoord in browsers kan voorkomen worden door de gebruikte browsers centraal te beheren. Ook dit maakt de omgeving echter complexer. Een andere mogelijkheid is het gebruik van het HTML-attribuut `autocomplete`. Hoewel dit attribuut in sommige gevallen genegeerd kan worden door moderne browsers zijn er mogelijkheden om het opslaan te voorkomen, zoals bijvoorbeeld het tijdelijk read-only maken van het wachtwoordveld of de browser altijd een nieuw wachtwoord te laten voorstellen.

[5] https://www.windowscentral.com/how-prevent-users-changing-proxy-settings-windows-10#disable_proxy_settings_windows10

3.3 Een beheerder kan zijn eigen wachtwoord wijzigen zonder dat daar het huidige wachtwoord voor nodig is



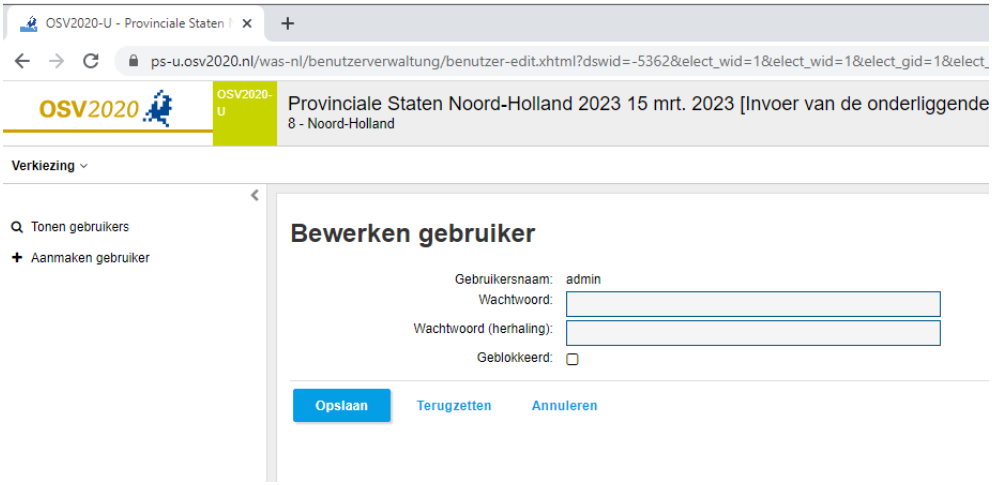


CVSS score	CVSS vector string
3.4 (Laag)	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L
ASVS categorie en richtlijn	
V2: Authentication, 2.1.6	

Bevinding

Binnen de applicatie is het voor gebruikers mogelijk om hun eigen wachtwoord te wijzigen. Daartoe dienen ze eerst hun oude wachtwoord in te geven daarna tweemaal het nieuwe, gewenste wachtwoord. Een gebruiker met de rol beheerder heeft daarnaast toegang tot het scherm gebruikersbeheer. De beheerder kan hier wachtwoorden van gebruikers wijzigen en accounts toevoegen, verwijderen en blokkeren. Voor deze handelingen is het niet nodig dat de beheerder zijn wachtwoord nogmaals invoert.

Een kwaadwillende medewerker die kortstondig toegang weet te verkrijgen tot de werkplek of gebruikerssessie van een beheerder kan daardoor bijvoorbeeld het wachtwoord van de beheerder zelf wijzigen zonder dat daarvoor het huidige wachtwoord nodig is, zoals weergegeven in Figuur 4. De kwaadwillende medewerker kan hiermee toegang krijgen tot een account met de rol “verkiezingsleider”, waarmee het verkiezingsproces beheerd kan worden en steminvoer kan worden goedgekeurd.



Figuur 4 - Het wijzigen van wachtwoord via gebruikersbeheer

Object(en)

Deze bevinding betreft de webinterface van OSV2020-U applicatie.

Risicoclassificatie

Wij classificeren de impact als midden. Een kwaadwillende medewerker die succesvol deze bevinding weet te misbruiken kan toegang krijgen tot een account met de rollen

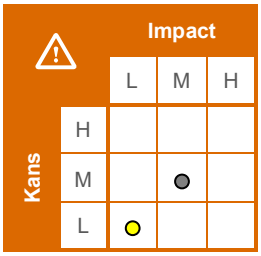
beheerder of leider. De beheerder rol kan gebruikt worden voor gebruikersbeheer maar heeft, op het verwijderen van de verkiezingsdefinitie binnen OSV2020-U na, geen invloed op het verkiezingsproces. Een account met de rol leider kan wel invloed op het proces uitoefenen. Een mogelijk scenario zou kunnen zijn dat een kwaadwillende medewerker zijn eigen (frauduleuze) invoer accepteert ten koste van de legitieme invoer van een andere medewerker. De impact hiervan wordt beperkt door de leidende rol die de papieren stemmen hebben binnen het overkoepelende verkiezingsproces.

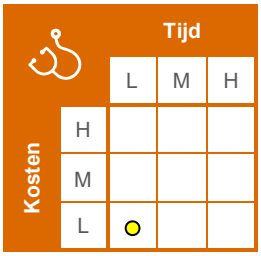
Een aanvaller heeft om misbruik te maken van de bevinding allereerst toegang nodig tot het netwerk waarop de applicatie beschikbaar is. In het geval van een kwaadwillende medewerker kan hiervan uit gegaan worden. Daarnaast is echter ook toegang nodig tot de werkplek of sessie van een beheerder. Hierdoor schatten wij de kans op misbruik in als laag.

Voorgestelde oplossing

Wij raden aan om te voorkomen dat een beheerder zijn eigen wachtwoord aan kan passen zonder dat daar het huidige wachtwoord voor nodig is.

3.4 Waarschuwingen over de aantallen en totalen van de getelde stemmen kunnen worden genegeerd waardoor mogelijk foutieve steminvoer kan worden geaccepteerd



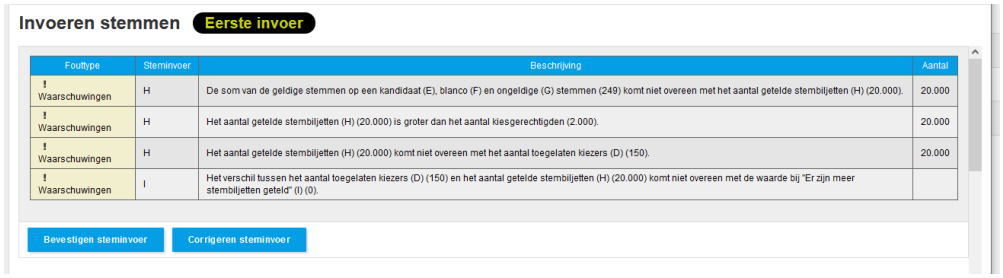


CVSS score	CVSS vector string
2.3 (Laag)	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N
ASVS categorie en richtlijn	
V11: Business Logic, 11.1.5	

Bevinding

De applicatie toetst de door de gebruiker ingevoerde aantallen stemmen, stembiljetten en overige zaken aan een aantal normen. Sommige van deze normen leveren een blokkerende melding op, waardoor de invoer niet opgeslagen kan worden. Een voorbeeld hiervan is dat de som van de aantallen stemmen op partijleden overeen moet komen met het totaal aantal stemmen op de partij.

Andere normen leveren echter alleen een waarschuwing op, zoals de check of het totaal aantal uitgebrachte stemmen groter is dan het aantal stembiljetten, of andersom. De gebruiker kan deze waarschuwing negeren en vervolgens de invoer opslaan. Figuur 5 geeft deze waarschuwing weer, inclusief de optie om de steminvoer te bevestigen.



Figuur 5 - Waarschuwing bij onlogische steminvoer

Object(en)

Deze bevinding is van toepassing op de webinterface van OSV2020-U.

Risicoclassificatie

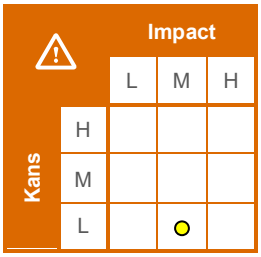
Wij classificeren de impact als laag. Een gebruiker kan de steminvoer bevestigen terwijl deze niet voldoet aan de normen. De mogelijkheid bestaat dat hierdoor foutieve steminvoer in OSV2020-U terechtkomt. Het risico wordt echter beperkt doordat twee gebruikers de aantallen stemmen onafhankelijk van elkaar moeten invoeren. Daarnaast is de impact in de context van het verkiezingsproces beperkt door de leidende rol van stemmen en stemaantallen op papier.

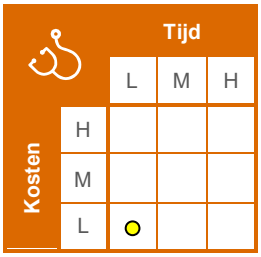
Wij classificeren de kans op misbruik als laag. Om misbruik te maken van de mogelijkheid foutieve steminvoer te accepteren zou een aanvaller toegang moeten hebben tot een account met de invoerrol en een account met de rol verkiezingsleider. Daarnaast bestaat er de mogelijkheid dat een gebruiker met de rol verkiezingsleider de waarschuwing (opzettelijk) negeert.

Voorgestelde oplossing

Wij raden aan de normen waaraan de stemaantallen moeten voldoen bindend te maken indien deze logisch gezien niet mogelijk zouden moeten zijn. In een situatie waarin een onrealistische aantallen zijn ingevoerd die niet voldoen aan de normen zou de waarschuwing verandert moeten worden in een blokkade om foutieve stemaantallen in OSV2020-U te voorkomen.

3.5 Een MySQL database gebruikt voor OSV2020-U wordt na verwijderen van de applicatie niet geleegd of verwijderd





CVSS score	CVSS vector string
3.0 (Laag)	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N
ASVS categorie en richtlijn	
N/A	

Bevinding

De OSV2020-U applicatie biedt de mogelijkheid gebruik te maken van een losse MySQL. De applicatie gebruikt de database voor het opslaan van applicatiegegevens zoals gebruikersaccounts, en voor het opslaan van verkiezingsgegevens zoals namen van stembureaus, kandidaten en aantallen stemmen als deze zijn ingevoerd.

Bij het verwijderen van de OSV2020-U applicatie wordt de database echter niet geleegd. Dit betekent dat een beheerder of gebruiker met directe toegang tot de database de gegevens later alsnog kan inzien. Eventuele persoonsgegevens in de database blijven dan ook beschikbaar na het verwijderen van de OSV2020-U applicatie, mogelijk tegen de verwachting van gebruikers van de applicatie in.

Hoewel gezien de context van de applicatie onwaarschijnlijk, kan dit ook gevolgen hebben als de applicatie nogmaals geïnstalleerd wordt met dezelfde database. Oude gegevens, zoals gebruikersaccounts, worden daarbij niet overschreven. Dit heeft als gevolg dat gebruikers van de oude installatie met hun inloggegevens kunnen inloggen in de nieuwe installatie. Een beheerder ziet deze accounts ook in het gebruikersbeheer staan en kan deze dan alsnog verwijderen.

Object(en)

Deze bevinding is van toepassing op de situatie waarin OSV2020-U gebruikt wordt met een losstaande database.

Risicoclassificatie

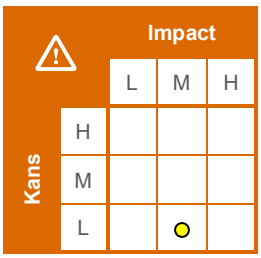
Wij classificeren de impact als midden. Het is mogelijk dat persoonsgegevens en andere verkiezingsdata tegen de verwachting van een beheerder in na deïnstallatie bewaard blijven in de database. Dit vergroot de kans dat deze data onbewust of als doelwit van een aanvaller in de openbaarheid komen.

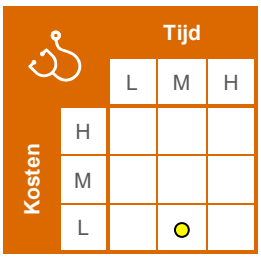
Wij classificeren de kans op misbruik als laag. Bij deïnstallatie van OSV2020-U wordt niet gewaarschuwd dat de data in de database niet wordt verwijderd. Ook in de handleiding wordt hier geen vermelding van gemaakt. De kans dat een dergelijke database niet wordt verwijderd is daardoor aanwezig. De Kiesraad heeft aangegeven dat de configuratie met een losstaande database echter niet vaak gebruikt wordt. Daarnaast moet een kwaadwillende gebruiker of aanvaller alsnog toegang krijgen tot het systeem waar de database op staat.

Voorgestelde oplossing

Wij raden aan de database van OSV2020-U tijdens de deïnstallatie van OSV2020-U op te schonen of te verwijderen. Hiermee wordt voorkomen dat mogelijk gevoelige data onbedoeld op systemen achterblijft.

3.6 Het is mogelijk om een sessiecookie in meerdere sessies tegelijkertijd te gebruiken

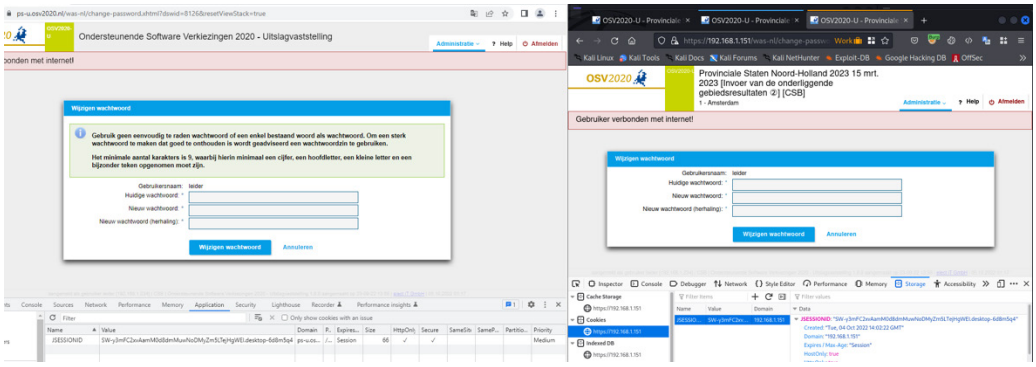




CVSS score	CVSS vector string
3.6 (Laag)	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N
ASVS categorie en richtlijn	
V3: Session Management, 3.3.4	

Bevinding

Voor de sessie tussen de eindgebruiker en de webserver van de applicatie wordt gebruikgemaakt van sessiecookies. Deze cookies, met de naam `JSESSIONID`, worden automatisch gegenereerd als een nieuwe client een verbinding met de webserver opzet en blijven geldig totdat de gebruiker uitlogt of de browser wordt gesloten. Een kwaadwillende gebruiker met toegang tot de browser van een andere gebruiker kan echter de cookie kopiëren en hergebruiken in zijn eigen browser. Op deze manier wordt toegang verkregen tot de sessie van de legitieme gebruiker. In Figuur 6 is te zien dat er twee sessies gelijktijdig actief zijn vanaf twee verschillende werkplekken, gebruikmakend van dezelfde sessiecookie.



Figuur 6 - Twee sessies met een identieke sessiecookie

Object(en)

Deze bevinding betreft configuratie van sessiemanagement binnen de webserver van de OSSV202-U applicatie.

Risicoclassificatie

Wij classificeren de impact als midden. Een aanvaller die een sessiecookie van een legitieme gebruiker weet te bemachtigen kan op deze manier toegang krijgen tot het account van de legitieme gebruiker. Binnen de applicatie krijgt de aanvaller dan dezelfde rechten als de legitieme gebruiker. Indien dit een account met de rol beheerder is, kan de aanvaller zichzelf blijvend toegang tot een account met meer rechten verschaffen. Zoals beschreven in 3.3 kan dit door het

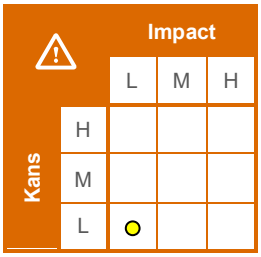
wachtwoord te wijzigen, zijn eventuele eigen account aan te passen naar de rol beheerder of een nieuw account met de rol beheerder aan te maken.

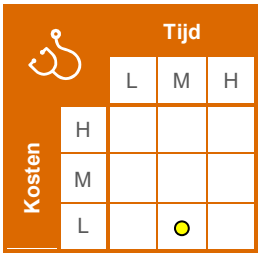
Wij classificeren de kans op misbruik als laag. Om misbruik te maken van deze bevinding dient een aanvaller een geldige sessiecookie te bemachtigen. Hiervoor moet een aanvaller toegang krijgen tot de werkplek en browser waarop de legitieme gebruiker is ingelogd, of een legitieme gebruiker overtuigen de sessiecookie te delen.

Voorgestelde oplossing

Wij raden aan sessiecookies, en daarmee sessies, te koppelen aan het IP-adres van gebruikers. Hierdoor is het niet meer mogelijk een gestolen sessiecookie vanaf een ander apparaat te gebruiken.

3.7 De OSV2020-U applicatie maakt gebruik van enkele verouderde en kwetsbare softwarecomponenten





CVSS score	CVSS vector string
3.6 (Laag)	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:L
ASVS categorie en richtlijn	
V14: Configuration, 14.2.1	

Bevinding

De OSV2020-U applicatie is gemaakt in Java en maakt gebruik van verschillende softwarecomponenten. Enkele van deze componenten zijn verouderd en bevatten bekende kwetsbaarheden. Tijdens het uitvoeren van de test is het niet gelukt om deze kwetsbaarheden uit te buiten doordat de kwetsbare delen van de componenten niet binnen de applicatie gebruikt worden, of omdat mitigerende maatregelen genomen zijn.

Voor het verwerken van XML-bestanden wordt gebruikgemaakt van Apache Xerces. De gebruikte versie van Xerces, 2.12.0.SP03, bevat een kwetsbaarheid waarmee mogelijk de beschikbaarheid van de applicatie beperkt kan worden[6]. Door bepaalde speciale karakters te gebruiken in zogenaamde XML internal entities en deze te uploaden naar een applicatie die gebruikmaakt van Xerces, kan een aanvaller de applicatie laten crashen. Het is echter niet gelukt OSV2020-U tijdens het onderzoek te laten crashen. Bij het verwerken van een XML-bestand met een internal entity geeft OSV2020-U aan dat de structuur van het bestand niet meer overeenkomt met de verwachte EML-structuur.

Daarnaast maakt de applicatie gebruik van Hibernate, een framework voor interactie tussen Java en een relationele database. De gebruikte versie, 5.3.24.Final, is in sommige situaties kwetsbaar voor SQL-injectie[7]. De kwetsbaarheid bevindt zich in het niet voldoende veilig verwerken van SQL literals in comments. Tijdens het testen is het niet gelukt deze kwetsbaarheid uit te buiten.

Object(en)

Deze bevinding heeft betrekking op de Java softwarecomponenten en frameworks die gebruikt worden door de OSV2020-U applicatie.

Risicoclassificatie

Wij classificeren de impact als laag. Indien een aanvaller de genoemde kwetsbaarheden succesvol weet uit te buiten heeft dit een beperkte impact op de applicatie. In het geval van de kwetsbaarheid in Xerces is het bij succesvol misbruik mogelijk dat de beschikbaarheid van de applicatie tijdelijk aangetast wordt. Succesvol misbruik van de kwetsbaarheid in Hibernate kan ertoe leiden dat een aanvaller (beperkt) inzicht krijgt in de data in de database.

Wij classificeren de kans op misbruik als laag. Voor beide kwetsbaarheden zijn mitigerende omstandigheden aanwezig. Daarnaast is voor het eventueel uitbuiten ervan ook toegang nodig tot een van de clients die toegang hebben tot de applicatie.

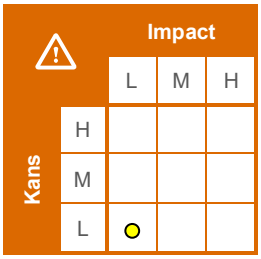
[6] CVE-2022-23437, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23437
[7] CVE-2020-25638, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25638

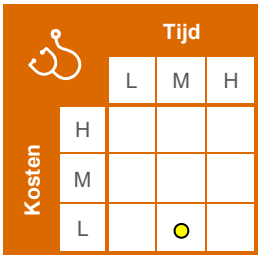
Voorgestelde oplossing

Wij raden aan de genoemde software bij te werken naar een nieuwere, niet kwetsbare versie. Voor Xerces is de meest recente versie 2.12.2[8]. Voor Hibernate is dit 6.1.4[9]. Wij raden verder aan voor alle gebruikte software(componenten) en frameworks (geautomatiseerd) te controleren of gebruik wordt gemaakt van een recente, niet-kwetsbare versie.

[8] https://mvnrepository.com/artifact/xerces/xercesImpl
[9] https://mvnrepository.com/artifact/org.hibernate.orm/hibernate-core

3.8 Directe aanpassingen in de database kunnen leiden tot inconsistenties tussen data die gebruikers zien in de front-end





CVSS score	CVSS vector string
2.3 (Laag)	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N
ASVS categorie en richtlijn	
N/A	

Bevinding

Aanpassingen in de database van OSV2020-U kunnen leiden tot inconsistenties in de webinterface van de applicatie. De situatie kan hierdoor ontstaan dat gebruikers voor hetzelfde object, zoals bijvoorbeeld het aantal getelde stembiljetten, verschillende waarden in hun webinterface zien. Zodra er directe aanpassingen gedaan zijn in de database kan hierdoor niet meer vertrouwd worden op de weergegeven getallen in de webinterface van de applicatie.

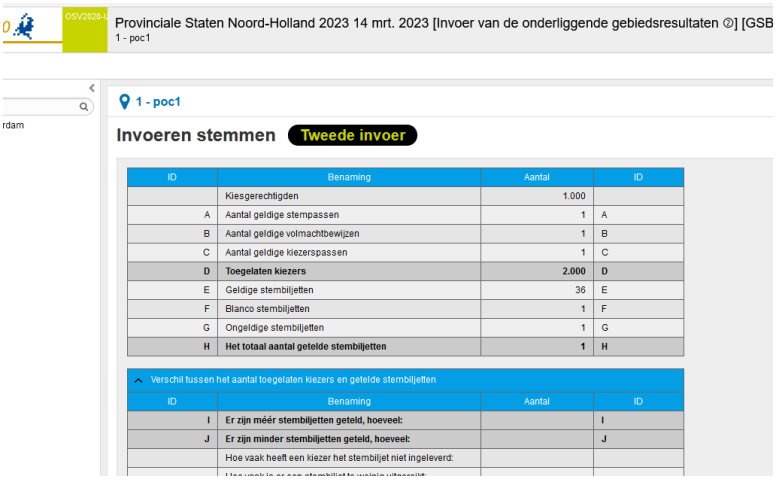
Figuur 7 laat het overzicht van de verkiezingsleider zien. Het aantal geldige stembiljetten onder de tweede steminvoer is 38. Figuur 8 laat het overzicht zien van de invoer gebruiker verantwoordelijk voor de tweede steminvoer. Het aantal geldige stembiljetten is in zijn overzicht 36. Deze inconsistentie blijft bestaan nadat de pagina's worden herladen.

ID	Benaming	Eerste steminvoer	Tweede steminvoer	ID
	Kiesgerechtigden	1.000	1.000	
A	Aantal geldige stempassen	1	1	A
B	Aantal geldige volmachtbewijzen	1	1	B
C	Aantal geldige kiezerspassen	1	1	C
D	**Toegelaten kiezers**	**2.000**	**2.000**	**D**
E	Geldige stembiljetten	50	38	E
F	Blanco stembiljetten	1	1	F
G	Ongeldige stembiljetten	1	1	G
H	**Het totaal aantal getelde stembiljetten**	**1**	**1**	**H**

Verschil tussen het aantal toegelaten kiezers en getelde stembiljetten

ID	Benaming	Eerste steminvoer	Tweede steminvoer	ID
I	**Er zijn méér stembiljetten geteld, hoeveel:**	**1**		**I**
J	**Er zijn minder stembiljetten geteld, hoeveel:**	**1**		**J**
	Hoe vaak heeft een kiezer het stembiljet niet ingeleverd:	1		
	Hoe vaak is er een stembiljet te weinig uitgereikt:	1		

Figuur 7 - Overzicht steminvoer verkiezingsleider



Figuur 8 - Overzicht tweede invoer

Object(en)

Deze bevinding betreft de interactie tussen de front-end en de database van de applicatie.

Risicoclassificatie

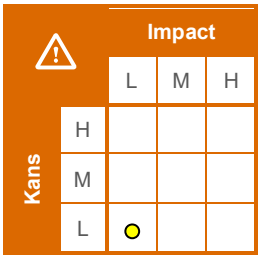
Wij classificeren de impact als laag. Het direct aanpassen van data in de database kan leiden tot inconsistenties in de applicatie. Mogelijk krijgen verschillende gebruikers hierdoor verschillende waarden te zien.

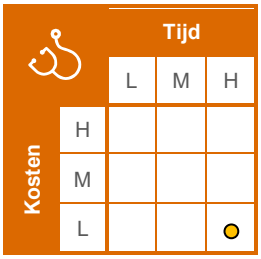
Het scenario beschreven in deze bevinding vereist dat een beheerder handmatig stemaantallen aanpast in de database. Wij classificeren de kans daardoor op laag.

Voorgestelde oplossing

Wij raden aan handmatige aanpassingen in de database te voorkomen. Uit overleg met de Kiesraad is gebleken dat de oorzaak van deze bevinding waarschijnlijk de gebruikte caching software is. Wij raden aan om te onderzoeken of een dergelijke inconsistentie in de weergegeven data ook kan ontstaan bij regulier gebruik van de applicatie.

3.9 Onnodige functionaliteit en data binnen de applicatie en database vergroten het aanvalsoppervlak van de applicatie

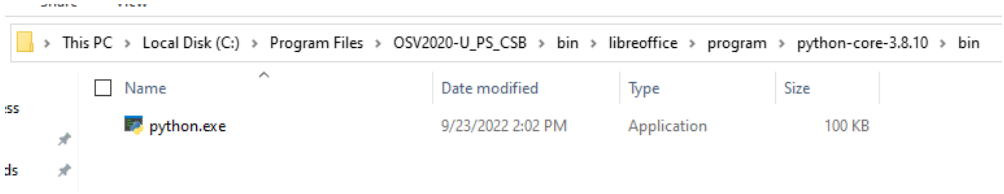




CVSS score	CVSS vector string
N/A	N/A
ASVS categorie en richtlijn	
V14.2 Dependency, 14.2.2	

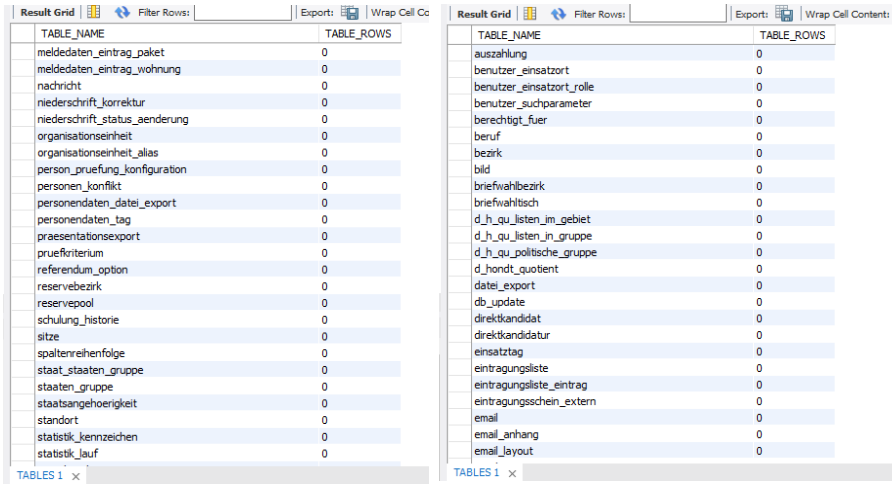
Bevinding

OSV2020-U bevat functionaliteit en aanvullende software die het aanvalsoppervlak van de applicatie en de omgeving waarin deze draait vergroten. Zo worden verschillende uitvoerbare bestanden meegeleverd met de applicatie. Een voorbeeld hiervan is een complete installatie van LibreOffice, dat op zijn beurt Python bevat, zoals te zien in Figuur 9. Deze versie van Python, 3.8.10, is daarnaast verouderd. In nieuwere versies zijn verschillende bugs en mogelijke kwetsbaarheden verholpen[10].



Figuur 9 - Python meegeleverd met LibreOffice

Daarnaast bevat ook de database veel tabellen die niet gebruikt worden bij het gebruik van OSV2020-U. Voorbeelden hiervan zijn weergegeven in Figuur 10.



Figuur 10 - Lege tabellen

[10] https://docs.python.org/release/3.8.15/whatsnew/changelog.html

Object(en)

Deze bevinding heeft betrekking op de applicatie, webinterface en database van OSV2020-U.

Risicoclassificatie

Deze bevinding leidt niet direct tot impact op OSV2020-U. Onnodige functionaliteit en meegeleverde software vergroten het aanvalsoppervlak van OSV2020-U. Een aanvaller met toegang tot het systeem waarop OSV2020-U kan bijvoorbeeld Python gebruiken om bepaalde restricties op het systeem te omzeilen. Deze versie van Python is daarnaast verouderd en bevat een kwestsbaarheid[11]. In de context van de OSV2020-U applicatie is deze kwetsbaarheid echter niet te misbruiken.

Wij classificeren de kans op misbruik als laag. Voordat misbruik mogelijk is dient een aanvaller alsnog een kwetsbaarheid te vinden in de betreffende functionaliteit of software. In het geval van de meegeleverde software heeft aanvaller eerst toegang nodig tot het systeem waarop OSV2020-U draait.

Voorgestelde oplossing

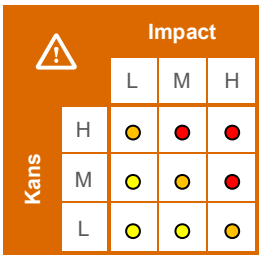
Wij raden aan de functionaliteit binnen OSV2020-U te beperken tot wat noodzakelijk is voor het doel van de applicatie. Daarnaast raden wij ook aan de software die meegeleverd wordt te beperken tot wat noodzakelijk is voor het functioneren van de applicatie. Tot slot adviseren wij na te gaan of software gebundeld met OSV2020-U bijgewerkt is tot de meest recente stabiele versie, en zo niet, deze te updaten.

[11] https://nvd.nist.gov/vuln/detail/CVE-2022-0391

A. Toelichting classificaties

A.1. Risico classificatie

Het risico wordt berekend op basis van de kans vermenigvuldigd met de impact. Bij elke gerapporteerde kwetsbaarheid maken wij een inschatting van de kans en impact inzichtelijk. Op basis van onderstaande risicomatrix:



Classificatie:

H Hoog
M Gemiddeld
L Laag

A.1.1. Kans

Bij het bepalen van de kans wordt rekening gehouden met het niveau dat is vereist om misbruik te maken een bevinding. Dit is mede afhankelijk van de beschikbaarheid van publiek beschikbare tools (exploits).

Classificatie	Omschrijving
Laag	Een aanvaller heeft ruime ervaring nodig op het gebied van hacking waarbij niet alleen gebruik wordt gemaakt van publiek toegankelijke tools.
Gemiddeld	Een aanvaller maakt indien nodig eenvoudige scripts om misbruik te maken van kwetsbaarheden.
Hoog	Een aanvaller heeft geen vergaande kennis nodig en kan met behulp van publiek beschikbare tools misbruik maken van kwetsbaarheden.

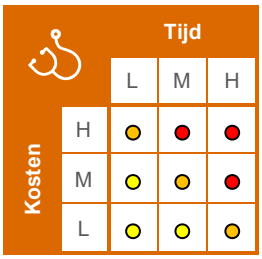
A.1.2. Impact

Bij het bepalen van de impact wordt rekening gehouden met de mate waarin een aanvaller door middel van het uitbuiten van de kwetsbaarheid ongeautoriseerde toegang kan hebben tot systemen en gegevens.

Classificatie	Omschrijving
Laag	De kwetsbaarheid levert niet een direct gevaar op voor de interne systemen, maar is een teken van een onvolledige beveiliging.
Gemiddeld	Een aanvaller kan door het misbruiken van een kwetsbaarheid niet direct ongeautoriseerd toegang verkrijgen maar kan in combinatie met andere hulpmiddelen of informatie, ongeautoriseerde toegang verkrijgen.
Hoog	Een aanvaller heeft ongeautoriseerd toegang tot de systemen en gegevens.

A.2. Inspanning classificatie

De inspanning wordt berekend op basis van de geschatte kostenbesteding vermenigvuldigd met de tijdsbesteding. Op basis van onderstaande matrix is de resulterende inspanning te bepalen.



Classificatie:

H Hoog
M Gemiddeld
L Laag

A.2.1. Kosten

Bij het bepalen van de kosten schatten wij in of een aanbeveling hoge kosten met zich meebrengt in het kader van hardware- of softwareaankopen.

Classificatie	Omschrijving
Laag	Er zijn geen hard- of softwarekosten benodigd. Een aanbeveling met een lage kosten classificatie betekent dat met de huidig aanwezige middelen de verbeteringen doorgevoerd kunnen worden.
Gemiddeld	Er zijn gemiddelde hard- en/of softwarekosten benodigd. Deze classificatie kan betreffen het aankopen van een server of een softwarelicentie.
Hoog	Er zijn hoge hard- en/of softwarekosten benodigd. Meestal betreft een hoge kosten classificatie het aankopen van omvangrijke nieuwe hardware of softwarelicenties.

A.2.2. Tijdsinvestering

De tijdsbesteding is een inschatten van de hoeveel tijd benodigd is door beheerders of leveranciers om de aanbeveling te effectueren.

Classificatie	Omschrijving
Laag	Een aanbeveling met een lage tijdsbesteding betekent dat de aanbeveling binnen enkele uren doorgevoerd kan zijn. Een lage tijdsbesteding komt typisch voor bij een quick-win.
Gemiddeld	De aanbeveling betreft een situatie waarin meer tijd benodigd is om de aanbeveling door te voeren, zoals het afstemmen met een softwareleverancier of het vaststellen van compatibiliteitsproblemen ten gevolge van het doorvoeren van de verbetering.
Hoog	Een hoge tijdsbesteding betreft een situatie waarin een groot onderzoeks-traject noodzakelijk is, voordat de aanbeveling doorgevoerd kan worden.

B. Disclaimer

Een onderzoek als dit is gebaseerd op een selectie van mogelijke veiligheidstesten, beschikbare tijd, onze ervaring en beschikbare tools. Het onderzoek geeft inzicht in mogelijke zwakke plekken en risico's op het moment van uitvoering van de test, maar geeft geen volledig zicht op alle zwakke plekken en risico's. Daarnaast kunnen zich, door technologische ontwikkelingen en nieuwe 'aanvalsmethoden', nieuwe risico's voordoen na het uitvoeren van onze werkzaamheden.

Op de rapportage kan niet door anderen worden gesteund aangezien anderen die niet op de hoogte zijn van het doel van de werkzaamheden de resultaten onjuist kunnen interpreteren. Wij stellen dit document uitsluitend op voor de Kiesraad als opdrachtgever, in overeenstemming met de opdrachtbevestiging.

In dit Rapport zijn het kader en de beperkingen van de uitgevoerde werkzaamheden expliciet vermeld. Het Rapport is uitsluitend ten behoeve van de belangen van de Kiesraad uitgebracht en heeft niet het oogmerk om voor andere doeleinden dan de daarin genoemde, te worden gebruikt. Op het Rapport kan derhalve niet door anderen dan de Kiesraad worden gesteund. Voor het gebruik van het Rapport door andere partijen dan de Kiesraad aanvaarden wij derhalve geen verantwoordelijkheid, zorgplicht of aansprakelijkheid - contractueel, op basis van onrechtmatige daad (inclusief nalatigheid) of anderszins.

PwC Advisory N.V. (hierna: PwC) heeft zich bij het opstellen van het Rapport (mede) gebaseerd op documenten en informatie zoals PwC die van verschillende partijen (inclusief de Kiesraad) heeft ontvangen (hierna: 'Informatie van Derden'). PwC heeft de Informatie van Derden gebruikt met de aanname dat deze informatie juist, volledig en niet misleidend is. De betrouwbaarheid van de Informatie van Derden is door PwC niet geverifieerd of vastgesteld. PwC heeft geen accountantscontrole uitgevoerd met betrekking tot de Informatie van Derden, noch een beoordeling gericht op het vaststellen van volledigheid en juistheid daarvan conform internationale audit- of reviewstandaarden. PwC verstrekt geen enkele expliciete of impliciete verklaring of garantie ten aanzien van de juistheid of volledigheid van de Informatie van Derden of de daaraan gerelateerde referenties in het Rapport.

U blijft te allen tijde zelf volledig verantwoordelijk voor eventuele op dit Rapport gebaseerde besluitvorming en/of beslissing(en). PwC aanvaardt geen enkele aansprakelijkheid jegens u en/of enige derde voor de gevolgen van enig handelen of nalaten door u en/of derden op basis van (de inhoud van) het Rapport en wijst iedere verantwoordelijkheid, zorgplicht en/of aansprakelijkheid - contractueel, op basis van onrechtmatige daad of anderszins- – ter zake af.

Dit document alsmede enig geschil voortvloeiende uit of verband houdend met (de inhoud van) het document worden uitsluitend beheerst door Nederlands recht.