

resill!on

Rapportage beveiligingsonderzoek

Abacus van de Kiesraad



Beveiligingsonderzoek

Abacus van de Kiesraad

Datum	Versie	Auteur	Opmerking
07-09-2026	0.1	Resillion	Initiële versie
07-09-2026	0.2	Resillion	Bevindingen toegevoegd
09-09-2026	0.3	Resillion	Aanpassingen na bespreking bevindingen
11-09-2026	0.4	Resillion	Algemene hoofdstukken
11-09-2025	0.5	Resillion	QA-reviewversie
11-09-2026	0.6	Resillion	Eerste conceptversie voor de Kiesraad
29-09-2026	1.0	Resillion	Definitieve versie

Tabel 1: Versiegeschiedenis.

Details	
Rapport	KIESR-2602.SEC.v1_0
Status	Definitief
Datum	29 september 2026
Auteurs	Resillion

Tabel 2: Details van het rapport.

Classificatie	
Bepaald door	[REDACTED]
Niveau	Openbaar

Tabel 3: Details van de classificatie.

Dit document is eigendom van Resillion. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in welke vorm of op welke wijze dan ook, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of anderszins, zonder voorafgaande schriftelijke toestemming van de rechthebbende. Uiteraard mag de Kiesraad als opdrachtgever van het onderzoek dit rapport voor eigen gebruik reproduceren.

Auteursrecht © 2026, Resillion, alle rechten voorbehouden.

Het keurmerk CCV Cyber Security Pen Test heeft betrekking op de kwaliteit van de uitgevoerde pentest en niet op het beveiligingsniveau van het geteste object of diens omgeving.



Managementsamenvatting

De Kiesraad heeft Resillion gevraagd een beveiligingsonderzoek uit te voeren op Abacus, middels een white-box aanpak. De software wordt gebruikt als ondersteuning bij het verwerken en optellen van verkiezingsresultaten en het genereren van documenten (processen-verbaal). Abacus genereert diverse bestanden, waaronder teluitslagen-bestanden. Deze bestanden worden gedeeld tussen diverse overheidslagen op het overdrachtsplatform van de Kiesraad.

De opdracht bestaat uit enkel een applicatieve beoordeling, waarvan de resultaten in dit report worden beschreven.

Omvang van de opdracht

De initiële scope van deze opdracht is gedefinieerd in het voorstel KIESR-2602.PRO.v1_0. Het bestaat uit hands-on testen en een codereview.

Dekkingsgraad

Over het algemeen geeft de test een goed beeld van het beveiligingsniveau van Abacus. Dit is in lijn met het verwachte niveau voor dit type test.

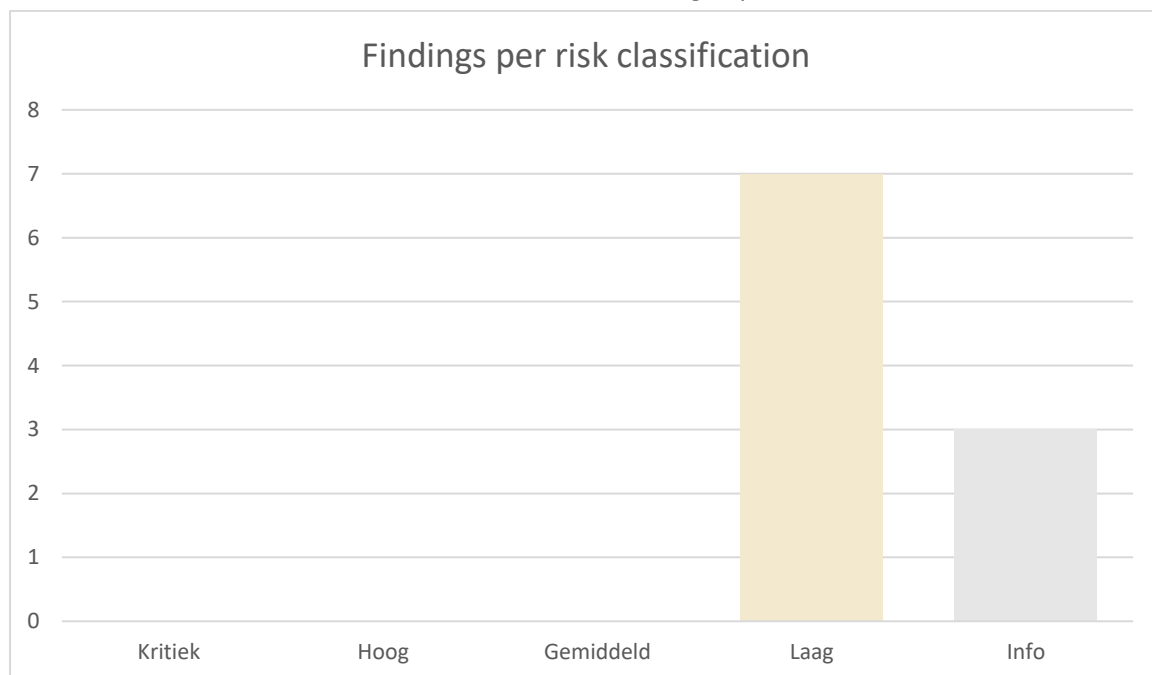
Beveiligingsonderzoeken zijn van nature tijdgebonden en worden uitgevoerd tijdens een vooraf bepaalde periode. Ze hebben betrekking op de geteste omgeving, zoals deze op het moment van de beoordeling werkt, met de kennis die op dat moment in het veld beschikbaar is.

Belangrijkste bevinding

Tijdens deze test zijn geen kwetsbaarheden gevonden met een kritiek, hoog of gemiddeld risico.

Classificaties van de bevindingen

In de onderstaande tabel staat het totaal aantal bevindingen per risicoclassificatie.



Figuur 1: Overzicht van bevindingen per risicoclassificatie.

Conclusie

Op basis van de bevindingen van het onderzoek is Resillion van mening dat het beveiligingsniveau van Abacus voldoet aan wat redelijkerwijs van moderne webapplicaties verwacht mag worden.

Het beveiligingsniveau van Abacus is eerder onderzocht, meest recent in februari 2026 door een andere leverancier van de Kiesraad. Het huidige onderzoek heeft een aantal nieuwe bevindingen opgeleverd ten opzichte van deze vorige test.

Tijdens het huidige onderzoek heeft Resillion de bevindingen van het eerdere onderzoek opnieuw beoordeeld. Daarbij is vastgesteld dat de belangrijkste bevindingen zijn opgelost, maar enkele bevindingen nog aanwezig zijn.

De gevonden kwetsbaarheden hebben voornamelijk betrekking op invoervalidatie en configuratie.

Er blijven enkele punten waarop de applicatie nog verbeterd kan worden, maar deze hebben niet in hebben kritieke of hoog-risico kwetsbaarheden geresulteerd. Dit komt voornamelijk doordat de applicatie alleen vanaf een *air-gapped* netwerk gebruikt wordt.

Op basis van de resultaten van dit onderzoek kunnen de grootste verbeteringen worden gerealiseerd door de invoervalidatie te verbeteren en de hardening van de Linux- en Windows-applicaties verder te versterken.

Onderzoeksvragen

Voorafgaand aan het security assessment heeft de Kiesraad een aantal testdoelen geformuleerd om potentiële veiligheidsrisico's te kunnen toetsen.

- In hoeverre zijn de installers vrij van plain tekst credentials of andere informatie waarvan het niet wenselijk is dat deze bekend raken?
Resillion heeft tijdens het onderzoek geen plain-tekst credentials of andere informatie aangetroffen waarvan het niet wenselijk is dat ze bekend zou raken.
- In hoeverre bevatten de installers andere ongewenste informatie/data (malware bijvoorbeeld)?
Resillion heeft tijdens het onderzoek geen ongewenste functionaliteit of software aangetroffen.
- In hoeverre is de software voldoende veilig om te gebruiken voor het doel (ondersteunen optellen van de resultaten en zetelberekening)?
Resillion concludeert dat de gevonden kwetsbaarheden binnen de context van het gebruiksdoel van de software (telondersteuning) een dermate klein risico vormen dat de software voldoende veilig kan worden geacht.

Inhoudsopgave

Managementsamenvatting	3
Inhoudsopgave	5
Figuurtabel.....	6
1 Afbakening en Aanpak	7
1.1 Scope van de opdracht	7
1.1.1 Onderzoek van de webapplicatie	7
1.1.2 Wijzigingen aan de omgeving	8
1.1.3 Beperkingen.....	8
1.2 Tooling	9
1.3 Onderwerp van dit document	9
1.4 Wijzigingen ongedaan maken.....	9
2 Glossarium	10
2.1 Verwijzingen	10
2.2 Termen en afkortingen	10
3 Bevindingen.....	11
3.1 Introductie	11
3.2 Classificatie: impact, waarschijnlijkheid en risico	11
3.2.1 Bevindingen en kwetsbaarheids-ID's.....	12
3.3 Bevindingen van de applicatietest.....	13
3.3.1 Invoerders kunnen willekeurige voortgangpercentages instellen	13
3.3.2 Geen controle of stembureaus bij verkiezingen horen	17
3.3.3 Archief met uitslag definitieve zitting kan verkeerde bestanden bevatten	21
3.3.4 Linux service niet optimaal gehard.....	23
3.3.5 Abacus voor Windows installeert in persoonlijke roaming folder.....	26
3.3.6 Geen limiet op het aantal inlogpogingen	28
3.3.7 Geen restricties op namen van gebruikers.....	30
3.3.8 Achterhalen van gebruikersnamen mogelijk met time-base enumeratie.....	33
3.3.9 <i>Air-gap</i> -detectie vereist geen “no route to host”	35
3.3.10 Voorspelbare <i>hash</i> -controle	37

Figuurtabel

Figuur 1: Overzicht van bevindingen per risicoclassificatie.	3
Figuur 2: De server accepteert 255 als geldig percentage.....	14
Figuur 3: geïmporteerde stembureaus.	18
Figuur 4: Succesvolle import.	19
Figuur 5: Logs bevatten ook geen foutmeldingen.	19
Figuur 6: Download van proces verbaal en telresultaat.	21
Figuur 7: Configuratie Windows installer.	26
Figuur 8: Brute-force op wachtwoordveld.....	28
Figuur 9: Aangepast request om gebruikersnaam met 4800+ karakters aan te maken.	30
Figuur 10: Gebruiker met lange gebruikersnaam is zichtbaar als valide account.	31
Figuur 11: Verschil in responsetijd bevestigt bestaan van gebruikersaccount.....	33
Figuur 12: selectie van de secties die de gebruiker moet invoeren.	37

1 Afbakening en Aanpak

1.1 Scope van de opdracht

In dit hoofdstuk worden de onderdelen van de opdracht beschreven. De informatie is gebaseerd op het voorstel[2], informatie die tijdens de voorbereiding is verstrekt (verzameld in het projectinitiatiedocument[3]), en eventuele wijzigingen die tijdens de uitvoering van het project zijn aangebracht. Testen worden uitgevoerd conform het CCV Keurmerk Pentesten.

Alle testwerkzaamheden zijn uitgevoerd tussen 31 augustus en 4 september.

1.1.1 Onderzoek van de webapplicatie

Het onderzoek richtte zich op het applicatiebeveiligingsniveau van Abacus en bestaat uit een handmatige test en een code review van de applicatie en een analyse van de installatiebestanden. De tests zijn uitgevoerd op basis van de OWASP ASVS¹ niveau 2.

Beoordeling van de code

Voor de code review is de volgende code aangeleverd.

Naam	Beschrijving	Checksum (SHA256)
abacus-1.1.0.zip	Broncode	d035ea5134169bfb025afb7449876a65fe22f2a8cfd3a74f1e13a9d2b8e6bbb6

Tabel 4: Overzicht van aangeleverde code.

Eventuele verschillen tussen deze code en de code die gebruikt is om de installatiebestanden samen te stellen, inclusief aanpassingen nadat de code is gedeeld voor de code-review, vallen niet binnen de scope van deze pentest.

Handmatig testen van de webapplicatie

De handmatige test op de Abacus webapplicatie is uitgevoerd op een lokale installatie op de testomgeving van Resillion. Testdata (zoals EML-bestanden) waren beschikbaar via de git repository².

Naam	Beschrijving	Checksum (SHA256)
abacus-linux-v1.1.0.tar.gz	Abacus voor Linux	ca4d5539e201f1645fc92599809264ddaf676e586d8d7802ac6cab21d5b57a16
abacus-windows-setup-v1.1.0.exe	Abacus voor Windows	7ec9b978b5b9395267afd3a2dd293826a6c69143c81d35c74198400b790a2ad3

Tabel 5: Overzicht van aangeleverde binaries.

De test is uitgevoerd vanuit de verschillende perspectieven die relevant zijn in de applicatie:

- Beheerder
- Coördinator (GSB / CSB)
- Invoerder
- Niet ingelogde gebruikers

Resillion had tijdens de test volledige controle over de omgeving en kon alle testdata en accounts zelf beheren.

Deel van het onderzoek is ook de configuratie van Abacus, zoals de TLS configuratie, de poorten die aan het netwerk ontsloten worden en de rechten die nodig zijn op het systeem.

1

<https://github.com/OWASP/ASVS/blob/master/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf>

² <https://github.com/kiesraad/abacus-documentatie/tree/main/gebruikersdocumentatie/src/testdocumenten>

Er zijn voor het inrichten van het onderliggende systeem en het netwerk waar Abacus wordt geïnstalleerd regels³ opgesteld. De testomgeving van Resillion is conform deze regels opgesteld. Risico's die voortkomen uit fouten in de configuratie van het onderliggende systeem vallen buiten de scope van het assessment.

Tijdens de het onderzoek is echter wel rekening gehouden met *defence-in-depth* maatregelen die in Abacus getroffen zouden kunnen worden om te beschermen tegen configuratiefouten in de onderliggende infrastructuur.

Hertest van bevindingen uit voorgaand onderzoek

Abacus is vorig jaar getest. Voorafgaand aan het onderzoek heeft de Kiesraad aangegeven daar de belangrijkste bevindingen van te hebben opgelost. Tijdens dit onderzoek zijn de bevindingen van de vorige keer opnieuw getest. De bevindingen die niet zijn opgelost zijn opnieuw in dit rapport opgenomen. Hieronder staan de opgeloste bevindingen.

Bevinding	Resultaat
A.1	Bevinding is technisch opgelost.
A.4	Bevinding is technisch opgelost.
A.6	Bevinding is technisch opgelost.
A.8	Bevinding is technisch opgelost.
A.10	Abacus gebruikt de data waar deze bevinding om gaat niet, maar het is onderdeel van de EML standaard.
A.11	De Kiesraad heeft aangegeven maatregelen getroffen te hebben die Resillion afdoende vindt.
A.12	Resillion vindt deze vorm van wachtwoord-hashing acceptabel voor het gebruiksscenario van Abacus.

Tabel 6: Overzicht van opgeloste bevindingen.

1.1.2 Wijzigingen aan de omgeving

Voor het uitvoeren van de test is geen testomgeving van de Kiesraad nodig geweest en er hoeft dus ook geen testconfiguratie of -data opgeruimd te worden, of toegang opgeheven te worden.

1.1.3 Beperkingen

Hoewel Resillion altijd probeert een volledig beeld te krijgen van alle kwetsbaarheden, blijkt het over het algemeen niet haalbaar om elk aspect van een applicatie volledig te beoordelen binnen een acceptabele budget- en tijdsbesteding. Er dient te worden beseft dat tijdens een pentest steekproefsgewijze controles worden uitgevoerd zoals in het voorstel van dit onderzoek omschreven.

Over het algemeen heeft een aanvaller meer tijd beschikbaar om een infrastructuur of applicatie te compromitteren. Het is daarom belangrijk dat men realiseert dat de kwetsbaarheden in dit rapport niet als een uitputtende lijst moeten worden beschouwd.

Overall waar kwetsbaarheden van een bepaald type worden gemeld, is het de verantwoordelijkheid van de Kiesraad om te controleren op vergelijkbare gevallen elders in de applicatie voorkomen.

Dit onderzoek wordt uitgevoerd binnen vooraf bepaalde budget- en tijdsgrenzen. Alle producten die in gebruik zijn, dienen ook na dit onderzoek up-to-date gehouden te worden, aangezien er in de loop der jaren waarschijnlijk nieuwe kwetsbaarheden aan het licht zullen komen.

³ <https://www.kiesraad.nl/verkiezingen/herindelingen/ondersteunende-software-herindelingsverkiezingen/gebruik-abacus-bij-uitslagvaststelling>

1.2 Tooling

De hands-on test is hoofdzakelijk uitgevoerd door middel van handmatige tests. Daarbij is de OWASP ASVS Level 2 gehanteerd als referentiekader, en is hoofdzakelijk gebruik gemaakt van Burp Suite⁴ als test tool.

Ook de code review is grotendeels handmatig uitgevoerd. Daarnaast is ter ondersteuning gebruik gemaakt van statische code analyse (Checkmarx⁵) en de AI-modellen Claude Sonnet en Opus.

Waar statische analyse goed is in het identificeren van kwetsbaarheden die te maken hebben met invoervalidatie en hard-coded secrets, is AI breder inzetbaar. Abacus heeft uitgebreide documentatie die gebruikt is als invoer om te verifiëren of de code doet wat er in die documentatie staat en om op basis van de combinatie van al deze informatie in kaart te brengen hoe belangrijke beveiligingsmechanismen zoals invoervalidatie, authenticatie en autorisatie werken. Op basis daarvan is AI vervolgens gebruikt om gericht te zoeken naar implementatiefouten en kwetsbaarheden in die mechanismen en of het waargenomen gedrag van de applicatie eisen of stellingen uit de documentatie kan ondermijnen.

Verder is voor het testen van de hardening gebruik gemaakt van Nessus⁶ en testssl⁷.

1.3 Onderwerp van dit document

Dit rapport beschrijft de resultaten, conclusies en aanbevelingen van het beveiligingsonderzoek. De bevindingen van de onderdelen zoals gedefinieerd onder 1.1.1, “Onderzoek van de webapplicatie” en zijn vooral relevant voor de ontwikkelaars van de applicatie.

1.4 Wijzigingen ongedaan maken

Het onderzoek is volledig uitgevoerd op de testomgeving van Resillion. Er zijn dus geen aanpassingen gemaakt in de omgeving van de Kiesraad die na de test opgeruimd zouden moeten worden.

⁴ <https://portswigger.net/burp>

⁵ <https://checkmarx.com>

⁶ <https://www.tenable.com/products/nessus>

⁷ <https://github.com/testssl/testssl.sh>

2 Glossarium

2.1 Verwijzingen

Ref.	Documentreferentie	Beschrijving
[1]	https://owasp.org/www-project-application-security-verification-standard/	OWASP Application Security Verification Standard.
[2]	KIESR-2602.PRO.v1_0	Voorstel
[3]	KIESR-2602.PID.v1_0	Project Initiatie Document
[4]	KIESR-2602.ATT.VVV	Nessus rapport de Kiesraad Abacus

Tabel 7: Referenties.

2.2 Termen en afkortingen

Term	Definitie
AI	Artificial Intelligence; kunstmatige intelligentie.
AP	Autoriteit Persoonsgegevens, de Nederlandse privacy-autoriteit.
ASVS	Application Security Verification Standard; standaard voor verificatie van applicatiebeveiliging.
AVG	Algemene Verordening Gegevensbescherming.
BRP	Basisregistratie Personen.
CAP	Linux capability; afzonderlijk toekenbare systeembevoegdheid.
CCV	Centrum voor Criminaliteitspreventie en Veiligheid.
CSB	Centraal stembureau.
CVSS	Common Vulnerability Scoring System; methode voor het classificeren van kwetsbaarheden.
EML	Election Markup Language; XML-standaard voor verkiezingsgegevens.
GSB	Gemeentelijk stembureau.
IDS	Intrusion Detection System; systeem dat netwerk- of systeemactiviteit controleert op verdachte patronen.
IPS	Intrusion Prevention System; systeem dat verdachte netwerk- of systeemactiviteit probeert te blokkeren.
JSON	JavaScript Object Notation; tekstformaat voor gestructureerde gegevensuitwisseling.
MAV	Modified Attack Vector; aangepaste CVSS-metrick voor de aanvalsroute.
OWASP	Open Worldwide Application Security Project.
PID	Project Initiatie Document.
PP	Politieke partijen; in dit document gebruikt voor het opstellen van een kandidatenlijst.
SHA256	Cryptografisch hash-algoritme uit de SHA-2-familie.
SSH	Secure Shell; protocol voor beveiligde toegang tot systemen op afstand.
SSL	Secure Sockets Layer, een verouderd versleuteld protocol, vervangen door TLS.
TLS	Transport Layer Security, een versleuteld protocol dat SSL vervangt.
URL	Uniform Resource Locator; adres van een resource op een netwerk.
XML	Extensible Markup Language; tekstformaat voor gestructureerde gegevens.
HTTP	Hypertext Transfer Protocol; protocol voor webverkeer.

Tabel 8: Termen en afkortingen.

3 Bevindingen

3.1 Introductie

In dit hoofdstuk worden de ruwe resultaten van de uitgevoerde tests samengevat. Er worden conclusies getrokken, kwetsbaarheden geclassificeerd en aanvullend worden passende aanbevelingen gedaan.

3.2 Classificatie: impact, waarschijnlijkheid en risico

Elke kwetsbaarheid is een bedreiging voor de organisatie. Om de juiste prioriteiten toe te kennen voor het selecteren van tegenmaatregelen om deze bedreigingen te beperken, is het belangrijk om aan elke kwetsbaarheid een risiconiveau toe te kennen. Het risiconiveau wordt bepaald door te kijken naar de verwachte impact wanneer een kwetsbaarheid zou worden uitgebuit en de kans (Kans) dat er misbruik zal plaatsvinden.

Het risiconiveau is het product van de impact en de Kans en wordt geclassificeerd met de niveaus informatief, laag, gemiddeld, hoog en kritiek.

Impact, Kans en risico worden hieronder verder toegelicht.

Impact

De impact geeft een idee van de omvang van de schade die het gevolg kan zijn van misbruik van de genoemde kwetsbaarheid.

Het is belangrijk om te beseffen dat de impact tweeledig kan zijn. Het misbruiken van een kwetsbaarheid heeft in eerste instantie een technische impact. Deze technische impact veroorzaakt in de meeste gevallen schade aan de organisatie van de Kiesraad. Denk hierbij aan reputatie- en/of financiële schade van juridische conflicten. Dit is de zogenaamde business impact.

Resillion classificeert de technische impact van elke kwetsbaarheid om de impact op de Kiesraad te bepalen.

Het impactniveau kan laag, gemiddeld of hoog zijn. Impact voor beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens die in de applicatie worden gebruikt, vormen de basis voor de classificatie. Aangezien de classificatie van de Kiesraad voor deze gegevens is van het grootste belang en Resillion niet op de hoogte is van deze classificatie, het niveau wordt bepaald op basis van professionele oordeelsvorming.

Waarschijnlijkheid

De waarschijnlijkheid geeft een indicatie van de waarschijnlijkheid dat de kwetsbaarheid daadwerkelijk wordt misbruikt en/of de waarschijnlijkheid dat de resultaten van de aanval enig nut hebben. De kans kan laag, gemiddeld of hoog zijn. Wanneer de kans groot is, wordt de kans op misbruik van een kwetsbaarheid als groot beschouwd.

Het toegekende niveau is gebaseerd op professionele oordeelsvorming en is onder andere gebaseerd op de volgende aspecten:

- De mogelijke aanvallers. Is de kwetsbaarheid alleen te misbruiken door lokale medewerkers of door iemand van het internet?
- Wat de motivatie van derden is om een kwetsbaarheid te ontdekken en uit te buiten. Aanvallers zullen normaal gesproken meer investeren in het vinden en misbruiken van een kwetsbaarheid in een applicatie voor internetbankieren dan in een informatieve website van een lokale winkelier.
- De kans dat een aanval succesvol is, kan sterk afhangen van externe factoren buiten de controle van een aanvaller. Dit kan ertoe leiden dat een kwetsbaarheid moeilijk te misbruiken is. De waarschijnlijkheid wordt in dit geval als beperkt beschouwd.
- Het verwachte ervaringsniveau van de aanvallers. Kan de kwetsbaarheid worden uitgebuit door een doorsnee computergebruiker, of zijn ervaren hackers nodig om iets te detecteren en uit te buiten?

Risico

Het totale 'gewicht' van een conclusie wordt geconsolideerd in het risiconiveau. Het risico geeft een indicatie van de urgentie waarmee de kwetsbaarheid moet worden aangepakt. Dit niveau is afgeleid van de combinatie van impact en waarschijnlijkheid.

Het risico wordt als Hoog of Kritiek ingeschat als volgens Resillion direct ingrijpen noodzakelijk is. Bevindingen zonder directe technische impact krijgen 'informatief' als classificatie.

De Kiesraad dient zelf te beslissen of er omstandigheden zijn waarvan Resillion mogelijk niet op de hoogte is die van invloed kunnen zijn op het risico op een kwetsbaarheid.

3.2.1 Bevindingen en kwetsbaarheids-ID's

Elke bevinding in dit rapport wordt geïdentificeerd aan de hand van de kwetsbaarheids-ID, een unieke ID die wordt toegewezen wanneer een bevinding voor het eerst wordt besproken. De titels van de bevindingen kunnen zijn gewijzigd tussen eerdere mededelingen en dit rapport. In die gevallen kan de kwetsbaarheids-ID worden gebruikt om specifieke kwetsbaarheden bij te houden. Bevindingen die niet eerder zijn gecommuniceerd, hebben een nieuwe kwetsbaarheids-ID.

3.3 Bevindingen van de applicatietest

In de volgende paragrafen worden alle bevindingen van de applicatietest beschreven.

3.3.1 Invoerders kunnen willekeurige voortgangpercentages instellen

Kwetsbaarheid ID	KIESR-2602-A01
Eerder gerapporteerd als	n.v.t.
Risico	Informatief

Bron

- /api/data_entries
- `backend/src/api/data\_entry.rs`

Beschrijving

De applicatie houdt tijdens de invoerfase bij hoe ver deze gevorderd is. Dit gebeurt mede op basis van *requests* die invoerders vanuit hun browser naar de server sturen. Wanneer een invoerder het proces start om resultaten in te voeren, staat in het *request* een voortgangpercentage. Als dit percentage door de invoerder wordt aangepast, krijgt de coördinator ook dit aangepaste percentage te zien in het overzicht. Dit zou misbruikt kunnen worden om vertrouwen in de telling te verlagen, of het invoerproces onder de 100 procent te houden.

Reproductie

Het bestand `backend/src/api/data\_entry.rs` bevat commentaar dat stelt dat voortgang tussen 0 en 100 mag zijn, en het is gedefinieerd als een u8 datatype:

```
/// Request structure for saving data entry
#[derive(Serialize, Deserialize, ToSchema, Clone, Debug, FromRequest)]
#[from_request(via(axum::Json), rejection(ApiError))]
#[serde(deny_unknown_fields)]
pub struct DataEntry {
    /// Data entry progress between 0 and 100
    #[schema(maximum = 100)]
    pub progress: u8,
    /// Data entry for a polling station
    pub data: Results,
    #[schema(value_type = Object)]
    /// Client state for the data entry (arbitrary JSON)
    pub client_state: ClientState,
}
```

Het OpenAPI schema (backend/openapi.json) doet hetzelfde:

```
"DataEntry": {
  "type": "object",
  "description": "Request structure for saving data entry",
  "required": [
    "progress",
    "data",
    "client_state"
  ],
  "properties": {
    "client_state": {
      "type": "object",
      "description": "Client state for the data entry (arbitrary JSON)"
    },
    "data": {
      "$ref": "#/components/schemas/Results",
      "description": "Data entry for a polling station"
    },
    "progress": {
      "type": "integer",
      "format": "int32",
      "description": "Data entry progress between 0 and 100",
      "maximum": 100,
    }
  }
}
```

```

    "minimum": 0
  },
},

```

De server controleert echter nergens of dat het geval is en accepteert daarom ook u8 waardes boven 100 (tot 255).

In hetzelfde bestand kopieert de onderstaande code de invoer van de gebruiker rechtstreeks in de `CurrentDataEntry` waarde zonder de inhoud te controleren:

```

let current_data_entry = CurrentDataEntry {
  progress: Some(data_entry_request.progress),
  user_id: user.id(),
  entry: data_entry_request.data,
  client_state: Some(data_entry_request.client_state),
};

// Transition to the new state
let new_state = match entry_number {
  EntryNumber::FirstEntry =>
    state.update_first_entry(current_data_entry)?,
  EntryNumber::SecondEntry =>
    state.update_second_entry(current_data_entry)?,
};

```

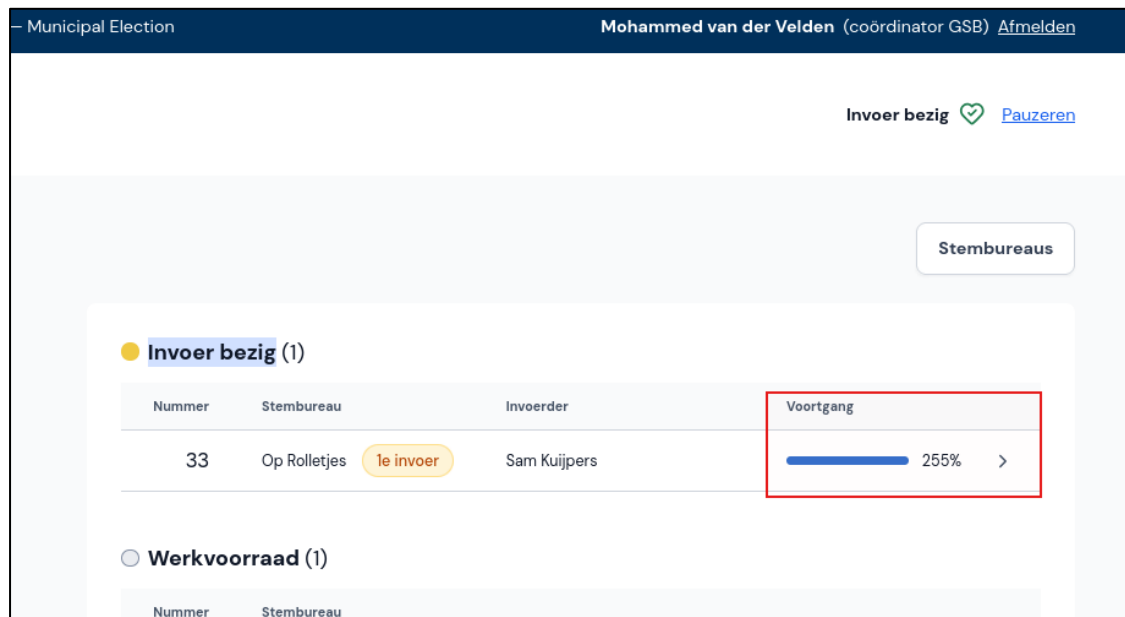
Om dit gedrag handmatig te controleren kunnen de onderstaande stappen gevolgd worden. Om dat te kunnen doen is een proxy zoals Burp Suite nodig om gemakkelijk netwerkverkeer aan te kunnen passen:

- 1) Log in met een 'invoerder GSB' account en ga naar een gemeentelijke verkiezing.
- 2) Kies een stembureau en klik op 'beginnen'.
- 3) Activeer de proxy om verkeer te onderscheppen en vul vervolgens bij de eerste stap 'nee' in bij beide vragen.
- 4) Vul in het onderschepte *request* de waarde '255' in voor de *progress*-parameter. Zet vervolgens de proxy weer uit.



Figuur 2: De server accepteert 255 als geldig percentage.

- 5) Log vervolgens in met een 'coördinator GSB' gebruiker en selecteer de gerelateerde verkiezing om de voortgang te bekijken.



Figuur 3: Coördinator krijgt ongeldig percentage te zien.

Impact: laag

Het telproces kan vertraagd worden.

Kans: gemiddeld

Iedere invoerder kan deze percentages aanpassen, maar er kan maar één persoon tegelijk resultaten invoeren voor een stembureau.

Risicoduiding

Gezien de ondersteunende rol van de software en het feit dat een coördinator tellingen opnieuw kan laten doen, zorgt dit ten hoogste voor vertraging of verwarring.

CVSS 4.0 score

Metrics	Scoring	Toelichting
Attack Vector (AV)	Network	De applicatie wordt gebruikt als webapplicatie over het netwerk.
Attack Complexity (AC)	Low	Er hoeven geen beveiligingsmaatregelen omzeild te worden.
Attack Requirements (AT)	Present	Er moet nog niemand anders bezig zijn met het invoeren van tellingen voor een stembureau.
Privileges Required (PR)	Low	Toegang als invoerder is benodigd.
User Interaction (UI)	None	Geen gebruikersinteractie nodig.
Confidentiality Impact (VC)	None	Er wordt geen (gevoelige) informatie prijsgegeven.
Integrity Impact (VI)	Low	Er wordt verkeerde informatie opgeslagen en aan de coördinator(s) getoond.
Availability Impact (VA)	None	Er is geen directe impact op beschikbaarheid.
Confidentiality Impact (SC)	None	Er is geen secundaire technische impact.
Integrity Impact (SI)	None	Er is geen secundaire technische impact.
Availability Impact (SA)	None	Er is geen secundaire technische impact.
Attack Vector (MAV)	Physical	Op verzoek van Kiesraad is de 'physical' MAV toegevoegd omdat zij stelt dat iedere gemeente aftekent op het gebruik van air-gapped systemen en netwerk waarin de software wordt gebruikt.

Metrics	Scoring	Toelichting
	Total score	Vector
	1.0	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/MAV:P

Aanbeveling

- Bepaal de voortgang op de server, op basis van al-ingevoerde gegevens.
- Beperk percentages tot waarden tussen 0 en 100.

3.3.2 Geen controle of stembureaus bij verkiezingen horen

Kwetsbaarheid ID	KIESR-2602-A02
Eerder gerapporteerd als	n.v.t.
Risico	Laag

Bron

- /api/elections/<ID>/polling_stations/validate-import
- `backend/src/api/polling\_station.rs`
- `backend/src/api/election.rs`
- `backend/src/eml/mod.rs`

Beschrijving

Een gebruiker met de 'GSB coördinator' rol kan bestanden voor een stemlokaal inladen die bij een andere verkiezing horen. Zo'n bestand bevat een identifier (of naam) voor de verkiezing en een datum. De applicatie controleert niet of de waardes in het bestand overeenkomen met de verkiezing die de coördinator had geselecteerd.

De geïmporteerde stemlokalen worden opgeslagen onder de verkeerde verkiezing. De auditlogfunctionaliteit slaat alle waardes wel correct op, maar registreert ook niet dat de identifier niet overeenkomt.

Reproductie

Volg deze stappen om de bevinding te bevestigen:

- 1) Log in als beheerder.
- 2) Stel een verkiezing in voor 2026, maar sla in het instellen van de stembureaus over.
- 3) Log uit.
- 4) Log in als coördinator van een gemeentelijk stembureau.
- 5) Kies de verkiezing uit stap 2.
- 6) Op het waarschuwingsscherm dat er nog geen stembureaus zijn ingesteld: kies 'stembureaus beheren' en klik de importeer optie.
- 7) Upload een voorbeeldbestand voor de gemeentelijke verkiezingen van 2022:

```
[...weggelaten voor leesbaarheid...]
<TransactionId>1</TransactionId>
<ManagingAuthority>
  <AuthorityIdentifier Id="0000">Test</AuthorityIdentifier>
  <AuthorityAddress/>
</ManagingAuthority>
<kr:CreationDateTime>2024-05-27T17:05:57</kr:CreationDateTime>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
c14n-20010315#WithComments"/>
<ElectionEvent>
  <EventIdentifier/>
  <Election>
    <ElectionIdentifier Id="GR2022_Test">
      <ElectionName>Gemeenteraad Test 2022</ElectionName>
      <ElectionCategory>GR</ElectionCategory>
      <kr:ElectionSubcategory>GR2</kr:ElectionSubcategory>
      <kr:ElectionDomain Id="0000">Test</kr:ElectionDomain>
      <kr:ElectionDate>2022-03-16</kr:ElectionDate>
      <kr:NominationDate>2022-01-31</kr:NominationDate>
    </ElectionIdentifier>
  <Contest>
    <ContestIdentifier Id="geen"/>
    <ReportingUnit>
      <ReportingUnitIdentifier Id="0000">Test</ReportingUnitIdentifier>
    </ReportingUnit>
    <VotingMethod>SPV</VotingMethod>
    <MaxVotes>612694</MaxVotes>
    <PollingPlace Channel="polling">
```

```

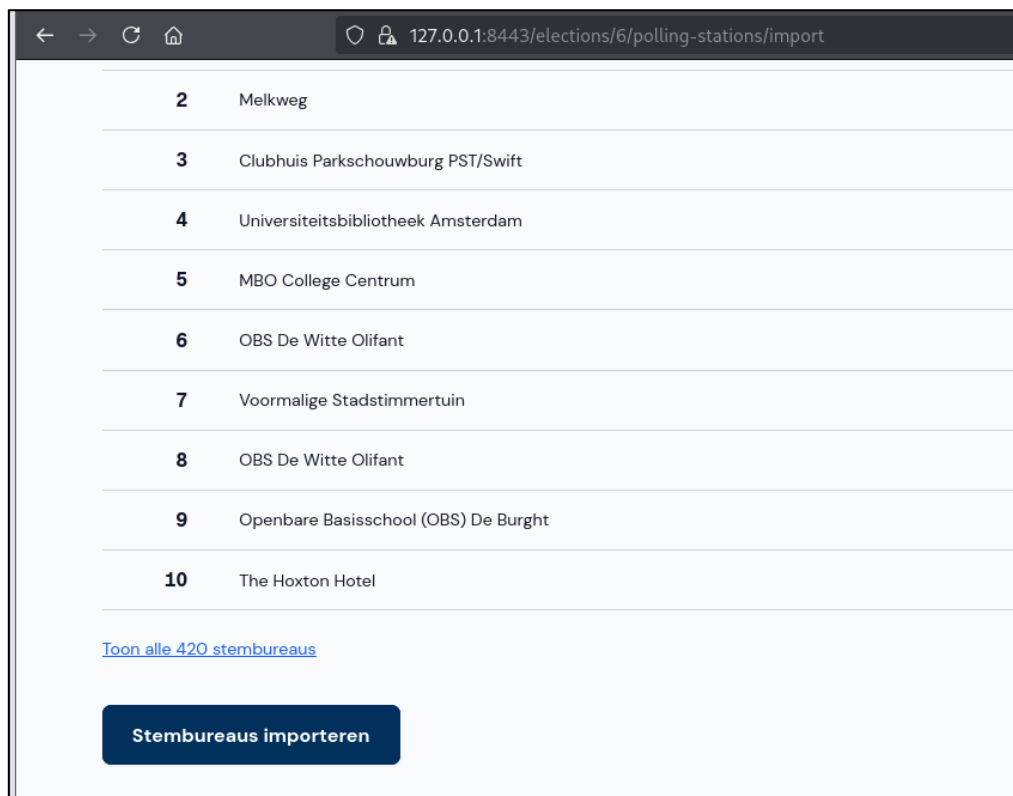
<PhysicalLocation>
  <Address>
    <Locality>
      <xal:LocalityName>Stadhuis</xal:LocalityName>
      <xal:PostalCode>
        <xal:PostalCodeNumber>1011 PN</xal:PostalCodeNumber>
      </xal:PostalCode>
    </Locality>
  </Address>
  <PollingStation Id="1">1273</PollingStation>
</PhysicalLocation>
</PollingPlace>

[...weggelaten voor leesbaarheid...]

</Contest>
</Election>
</ElectionEvent>
</EML>

```

De applicatie toont wel de geïmporteerde stembureaus, maar laat geen foutmelding zien dat de datum en de naam van de verkiezing niet klopt:



Figuur 3: geïmporteerde stembureaus.

- 8) Klik importeren. Merk op dat de stembureaus succesvol worden geïmporteed.

← → ↻ 🏠 127.0.0.1:8443/elections/6/polling-stations

GSB 0123 KleinDorp — Nieuwe Verkiezing

Stembureaus beheren

👍 Er zijn 420 stembureaus geïmporteerd

+ Stembureau toevoegen

Nummer	Naam
1	Stadhuis
2	Melkweg

Figuur 4: Succesvolle import.

- 9) Controleer het activiteitenlog en merk op dat de logs ook geen melding bevatten dat de naam en datum van de verkiezing niet kloppen:

Activiteitenlog

🔍 Filteren

Nummer	Tijdstip	Type
241	7 sep om 08:15	Succes
240	7 sep om 08:15	Succes
239	7 sep om 08:02	Informatie
238	7 sep om 07:42	Succes
237	2 sep om 09:35	Waarschuwing
236	2 sep om 09:31	Waarschuwing
235	2 sep om 09:31	Waarschuwing
234	2 sep om 09:31	Waarschuwing

Tijdstip
maandag 7 september 2026 om 08:15

Gebruikersnaam
ab_coordinator_1

Volledige naam
Mohammed van der Velden

Rol
coördinator GSB

Gebruikers-ID
3

Toelichting
Polling stations file hash: d430 c6f3 1de7 dade dea2 f9b0 072a a040 222c 3a17 745b 44d6 efi2 a777 0052 6c00

IP-adres
::ffff:127.0.0.1

Details

Verkiezings-ID
6

Bestandsnaam
source-election.eml.xml

Aantal geïmporteerde stembureaus
420

Figuur 5: Logs bevatten ook geen foutmeldingen.

Impact: laag

Een GSB coördinator kan een syntactisch geldig bestand van een andere verkiezing koppelen, zonder duidelijke waarschuwing of melding in de *audit trail*. Dit brengt het proces niet echt in gevaar, maar kan wel voor wat vertraging zorgen.

Kans: gemiddeld

Toegang als coördinator is benodigd. Een verkiezing moet nog geen stembureaus gekoppeld hebben.

Risicoduiding

Gezien de ondersteunende rol van de software zorgt dit ten hoogste voor vertraging of verwarring.

CVSS 4.0 score

Metrics	Scoring	Toelichting
Attack Vector (AV)	Network	De applicatie wordt gebruikt als webapplicatie over het netwerk.
Attack Complexity (AC)	Low	Er hoeven geen beveiligingsmaatregelen omzeild te worden en een syntactisch juist bestand volstaat.
Attack Requirements (AT)	Present	Een verkiezing moet nog geen stembureaus gekoppeld hebben
Privileges Required (PR)	Low	Toegang als coördinator is benodigd.
User Interaction (UI)	None	Geen gebruikersinteractie nodig.
Confidentiality Impact (VC)	None	Er wordt geen (gevoelige) informatie prijsgegeven.
Integrity Impact (VI)	Low	Er wordt verkeerde informatie opgeslagen.
Availability Impact (VA)	None	Er is geen directe impact op beschikbaarheid.
Confidentiality Impact (SC)	None	Er is geen secundaire technische impact.
Integrity Impact (SI)	None	Er is geen secundaire technische impact.
Availability Impact (SA)	None	Er is geen secundaire technische impact.
Attack Vector (MAV)	Physical	Op verzoek van Kiesraad is de 'physical' MAV toegevoegd omdat zij stelt dat iedere gemeente aftekent op het gebruik van air-gapped systemen en netwerk waarin de software wordt gebruikt.
	Total score	Vector
	1.0	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/MAV:P

Aanbeveling

- Controleer bij importeren of de gegevens van het geïmporteerde bestand wel passen bij de geselecteerde verkiezingen.
- Laat in het *audit-trail* duidelijk zien wanneer geïmporteerde stembureaus niet bij de verkiezing passen.

3.3.3 Archief met uitslag definitieve zitting kan verkeerde bestanden bevatten

Kwetsbaarheid ID	KIESR-2602-A03
Eerder gerapporteerd als	n.v.t.
Risico	Informatief

Bron

- /api/elections/<ELECTION_ID>/committee_sessions/<SESSION_ID>/download_zip_results
- `backend/src/api/report.rs`

Beschrijving

Na de definitieve zitting downloadt de coördinator een zipbestand met het proces-verbaal en de ondersteunende bestanden met telresultaten. Het *request* om dit bestand te downloaden bevat een *identifier* van een verkiezing en een zitting. Abacus controleert niet of deze twee bij elkaar horen en genereert een archief met de aangegeven informatie, waardoor willekeurige combinaties gemaakt kunnen worden.

Reproductie

Volg de onderstaande stappen om dit gedrag te bevestigen. Er zijn meerdere verkiezingen met afgeronde invoerfase en zitting nodig.

- 1) Log in als coördinator van een gemeentelijk stembureau.
- 2) Ga naar één van de verkiezingen.
- 3) Gebruik een proxy zoals Burp Suite om de URL van het volgende *request* te kunnen zien.
- 4) Klik de downloadknop.
- 5) Zoek in de proxy het *request* van deze download op en herhaal deze met een andere verkiezingsidentificatie.

```
GET /api/elections/5/committee_sessions/5/download_zip_results HTTP/1.1
Host: 127.0.0.1:8443
Cookie: ABACUS_SESSION=dgSu4RUgSw0vsX7bVkkq2AWA
[...weggelaten voor leesbaarheid...]
```

Het *request* ziet er dan als volgt uit:

<pre>GET /api/elections/7/committee_sessions/5/download_zip_results HTTP/1.1 Host: 127.0.0.1:8443 Cookie: ABACUS_SESSION=dgSu4RUgSw0vsX7bVkkq2AWA User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate, br Upgrade-Insecure-Requests: 1 Sec-Fetch-Dest: document Sec-Fetch-Mode: navigate Sec-Fetch-Site: same-origin Sec-Fetch-User: ?1 X-Pwntox-Color: blue Priority: u=0, i Te: trailers Connection: keep-alive</pre>	<pre>1 HTTP/1.1 200 OK 2 content-type: application/zip 3 content-disposition: attachment; filename="definitieve-documenten_gr2026_othertown_gemeente_oth 4 x-session-expires-at: 2026-09-07T14:35:55.392575113+00:00 5 cache-control: no-store 6 cross-origin-opener-policy: same-origin 7 cross-origin-embedder-policy: require-corp 8 cross-origin-resource-policy: same-origin 9 x-permitted-cross-domain-policies: none 10 x-content-type-options: nosniff 11 x-frame-options: deny 12 strict-transport-security: max-age=31536000; includeSubDomains 13 date: Mon, 07 Sep 2026 14:11:06 GMT 14 Content-Length: 77807 15 16 PKCq'j& 17 czx\$yWModel_Na31-2.pdfä} EÜAPl(ë+q0"\$ÜRB#FÄ#YÄAr/P*cD*qX 18 TD)JS@AÄüyfçU»YÜii,Çñ6}7UİpyE>36ügôİëDİ«5.İ¶Ün«VE 19 VEI>E`i 8*], \$E-ÜwWÄ*xex8İø7-DäEoA6-P9Eeİh3Zx0¶jUMâa*\ti@DE`\$*>6</pre>
---	---

Figuur 6: Download van proces verbaal en telresultaat.

Het archief dat gedownload wordt bevat echter de naam van de verkiezing waar de zitting bij hoort.

Impact: low

Het gedownloade archief kan de verkeerde informatie bevatten. Deze informatie is niet kwaadaardig en bevat geldige informatie voor een andere verkiezing.

Kans: low

Toegang als coördinator is benodigd. Een verkiezing moet een geldige, voltoide, zitting hebben en er moeten meerdere verkiezingen met telbestanden aanwezig zijn.

Risicoduiding

Gezien de ondersteunende rol van de software zit Resillion geen aanvalsscenario om hier misbruik van te maken.

CVSS 4.0 score

Metrics	Scoring	Toelichting
Attack Vector (AV)	Network	De applicatie wordt gebruikt als webapplicatie over het netwerk.
Attack Complexity (AC)	Low	Er hoeven geen beveiligingsmaatregelen omzeild te worden.
Attack Requirements (AT)	Present	Een verkiezing moet een geldige, voltooide, zitting hebben en er moeten meerdere verkiezingen met telbestanden aanwezig zijn.
Privileges Required (PR)	Low	Toegang als coördinator is nodig.
User Interaction (UI)	None	Geen gebruikersinteractie nodig.
Confidentiality Impact (VC)	None	Er wordt geen (gevoelige) informatie prijsgegeven, want een coördinator heeft al toegang tot al deze data.
Integrity Impact (VI)	Low	Er wordt verkeerde informatie opgeslagen.
Availability Impact (VA)	None	Er is geen directe impact op beschikbaarheid.
Confidentiality Impact (SC)	None	Er is geen secundaire technische impact.
Integrity Impact (SI)	None	Er is geen secundaire technische impact.
Availability Impact (SA)	None	Er is geen secundaire technische impact.
Attack Vector (MAV)	Physical	Op verzoek van Kiesraad is de 'physical' MAV toegevoegd omdat zij stelt dat iedere gemeente aftekent op het gebruik van air-gapped systemen en netwerk waarin de software wordt gebruikt.
	Total score	Vector
	1.0	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/MAV:P

Aanbeveling

Baseer het archief puur op de *identifiser* van de zitting, of controleer op de server of de aangegeven zitting bij de aangegeven verkiezing hoort.

3.3.4 Linux service niet optimaal gehard

Kwetsbaarheid ID	KIESR-2602-A04
Eerder gerapporteerd als	n.v.t.
Risico	Informatief

Bron

- abacus.service (Linux service definition file)

Beschrijving

De Abacus applicatie kan op een Linux system als service worden uitgevoerd. Hiervoor wordt door de Kiesraad een service file geleverd welke redelijk is gehard, maar die verder kan worden verbeterd:

- *CapabilityBoundingSet=CAP_NET_BIND_SERVICE* is niet ingesteld. Hoewel *AmbientCapabilities* is ingesteld, worden de *capabilities* hiermee niet beperkt tot uitsluitend het *binden* aan TCP- of UDP-poorten onder 1024.
- *SystemCallFilter* is niet ingesteld en blokkeert daarom geen system calls zoals mount of ptrace.
- *PrivateDevices=true* is niet ingesteld. Hierdoor wordt de toegang tot fysieke apparaten, zoals bijvoorbeeld */dev/sda* of */dev/mebm*, niet geblokkeerd.
- *ProtectClock=true* is niet ingesteld. Hierdoor wordt bijvoorbeeld het wijzigen van de systeemtijd niet geblokkeerd, wat gevolgen kan hebben voor TLS-verbindingen of tijdstempels in logging.
- *ProtectKernelLogs* is niet ingesteld op *true*. Door dit niet in te stellen, behoudt de service leestoeegang tot informatie uit de kernellogboeken.
- *ProtectHostname=true* is niet ingesteld. Door dit in te stellen wordt voorkomen dat de service de hostnaam of domeinnaam van het systeem kan wijzigen.
- *ProtectProc=invisible* is niet ingesteld. Hierdoor zijn de processen van andere gebruikers niet verborgen voor de Abacus-service.
- *ProcSubset=pid* is niet ingesteld. Hierdoor heeft de service toegang tot alle proc-interfaces, zoals */proc/sys* of */proc/keys*.

Reproductie

Bekijk om het bestaan van dit probleem te verifiëren de huidige inhoud van abacus.service:

```
[Unit]
Description=Abacus
After=network.target
Wants=network.target

[Service]
Type=exec
ExecStart=/usr/local/bin/abacus
DynamicUser=true
StateDirectory=abacus
WorkingDirectory=%S/abacus
Restart=always
RestartSec=5
StartLimitInterval=60
StartLimitBurst=3
AmbientCapabilities=CAP_NET_BIND_SERVICE
NoNewPrivileges=true
ProtectSystem=strict
ProtectHome=true
PrivateTmp=true
ProtectKernelTunables=true
ProtectKernelModules=true
ProtectControlGroups=true
RestrictSUIDSGID=true
RestrictRealtime=true
```

```

RestrictNamespaces=true
LockPersonality=true
MemoryDenyWriteExecute=true
SystemCallArchitectures=native
UMask=0077
StandardOutput=journal
StandardError=journal
SyslogIdentifier=abacus

[Install]
WantedBy=multi-user.target

```

De genoemde verbeteringen ontbreken in de huidige versie van deze file.

Impact: low

De huidige configuratie met het aangeleverde bestand *abacus.service* is niet per definitie onveilig. De genoemde verbeteringen worden uitsluitend beschouwd als aanvullende maatregelen voor *defence-in-depth*.

Kans: low

Omdat er in de huidige configuratie geen beveiligingsproblemen aanwezig zijn, wordt de waarschijnlijkheid als laag ingeschat.

Risicoduiding

Gezien er in de huidige situatie geen onveilige configuratie in gebruik is, is het risico van deze bevinding extreem laag en daarom ingeschaald als informatief.

CVSS 4.0 score

Metrics	Scoring	Toelichting
Attack Vector (AV)	Network	De applicatie wordt gebruikt als webapplicatie over het netwerk.
Attack Complexity (AC)	Low	Misbruik maken van deze misconfiguraties is eenvoudig als er eenmaal een andere kwetsbaarheid gevonden is.
Attack Requirements (AT)	Present	Er zijn andere kwetsbaarheden nodig om misbruik te maken van de misconfiguraties.
Privileges Required (PR)	None	Hangt af van de gevonden kwetsbaarheid. In het ergste geval is er geen authenticatie nodig.
User Interaction (UI)	None	Geen interactie met andere gebruikers nodig.
Confidentiality Impact (VC)	Low	In sommige gevallen kan informatie van het systeem uitgelezen worden
Integrity Impact (VI)	Low	Systeemeigenschappen kunnen aangepast worden.
Availability Impact (VA)	High	De applicatie kan onbereikbaar worden gemaakt.
Confidentiality Impact (SC)	None	Er is geen secundaire technische impact.
Integrity Impact (SI)	None	Er is geen secundaire technische impact.
Availability Impact (SA)	None	Er is geen secundaire technische impact.
Attack Vector (MAV)	Physical	Op verzoek van Kiesraad is de 'physical' MAV toegevoegd omdat zij stelt dat iedere gemeente aftekent op het gebruik van air-gapped systemen en netwerk waarin de software wordt gebruikt.
	Total score	Vector
	4.4	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N/MAV:P

Aanbeveling

Verbeter de beveiliging van de installatie door de volgende instellingen toe te voegen aan of aan te passen in het bestand *abacus.service*. Wijzigingen moeten grondig worden getest om te verifiëren dat ze geen nadelige gevolgen hebben voor de functionaliteit van de service voordat ze in productie worden geïmplementeerd:

- *CapabilityBoundingSet=CAP_NET_BIND_SERVICE*
- *SystemCallFilter=@system-service* (of overweeg een meer toegespitste samengestelde lijst)
- *PrivateDevices=true*
- *ProtectClock=true*
- *ProtectKernelLogs=true*
- *ProtectHostname=true*
- *ProtectProc=invisible*
- *ProcSubset=pid*

3.3.5 Abacus voor Windows installeert in persoonlijke roaming folder

Kwetsbaarheid-ID	KIESR-2602-A05
Eerder gerapporteerd als	n.v.t.
Risico	Laag

Bron

- Abacus voor Windows

Beschrijving

De Abacus-installatiebestanden voor Windows zijn zo geconfigureerd dat Abacus per gebruiker in 'userappdata' wordt geïnstalleerd. Dit betekent dat de applicatie in de roaming folder terecht komt, waar de gebruiker zelf de inhoud van de applicatie- en datafolders kan aanpassen en dat bij een misconfiguratie waardoor de air-gap (tijdelijk) wegvalt, de inhoud van de roaming folder automatisch overschreven of gesynchroniseerd kan worden via internet.

Bewijs

packaging\windows\abacus.iss bevat de volgende configuratie:

```
abacus-1.1.0 > packaging > windows > abacus.iss
21 [Setup]
22 ; NOTE: The value of AppId uniquely identifies this application. Do not use the same AppId
23 ; (To generate a new GUID, click Tools | Generate GUID inside the IDE.)
24 AppId={{8475448A-D5A3-4114-BD32-CDE54A5E2FB5}}
25 AppName={#MyAppName}
26 AppVersion={#GetVersion()}
27 AppPublisher={#MyAppPublisher}
28 AppPublisherURL={#MyAppURL}
29 AppSupportURL={#MyAppURL}
30 AppUpdatesURL={#MyAppURL}
31 DefaultDirName={userappdata}\{#MyAppName}
32 ; Setup will not show the Select Destination Location wizard page.
33 DisableDirPage=yes
34 ; "ArchitecturesAllowed=x64compatible" specifies that Setup cannot run
35 ; on anything but x64 and Windows 11 on Arm.
36 ArchitecturesAllowed=x64compatible
37 ; "ArchitecturesInstallIn64BitMode=x64compatible" requests that the
38 ; install be done in "64-bit mode" on x64 or Windows 11 on Arm,
39 ; meaning it should use the native 64-bit Program Files directory and
40 ; the 64-bit view of the registry.
41 ArchitecturesInstallIn64BitMode=x64compatible
42 DisableProgramGroupPage=yes
43 PrivilegesRequired=lowest
44 OutputBaseFilename=abacussetup
```

Figuur 7: Configuratie Windows installer.

Impact: hoog

Een kwetsbaarheid in de applicatie zorgt ervoor dat de aanvaller genoeg rechten heeft op het systeem om de werking van de applicatie aan te passen, of de database zelf.

In het geval dat de air-gap (tijdelijk) wegvalt en de beheerder geen lokaal account heeft gebruikt, kan de inhoud van de installatiefolder, inclusief database, gesynchroniseerd worden. Daarbij kunnen gegevens verloren gaan, of in een gericht aanvalsscenario de applicatie of database op de server worden vervangen met kwaadaardige versies.

Kans: laag

Deze misconfiguratie is niet direct uitbuitbaar, omdat voor beide scenario's eerst iets ander verkeerd moet gaan. Zo moet de applicatie andere kwetsbaarheden bevatten die toegang tot het onderliggende

systeem bieden voordat een aanvaller toegang heeft of moet de beheerder zijn persoonlijke account gebruikt hebben en het systeem tegen instructies in toch aan het netwerk gekoppeld hebben in het scenario dat de air-gap wegvalt.

Risicoduiding

Tijdens het onderzoek zijn geen kwetsbaarheden aangetroffen die tot dit soort misbruik kunnen leiden. Daarnaast moet de beheerder die de applicatie heeft geïnstalleerd ook een minder veilige route hebben gekozen om het met diens eigen account te installeren. Het uiteindelijke risico is daarom laag.

CVSS 4.0 score

Metrics	Scoring	Toelichting
Attack Vector (AV)	Network	De applicatie wordt gebruikt als webapplicatie over het netwerk.
Attack Complexity (AC)	Low	Misbruik maken van hoge rechten is eenvoudig als er eenmaal een andere kwetsbaarheid gevonden is.
Attack Requirements (AT)	Present	Er zijn andere kwetsbaarheden nodig om misbruik te maken van de hogere rechten. De beheerder moet diens eigen account gebruikt hebben.
Privileges Required (PR)	None	Hangt af van de gevonden kwetsbaarheid. In het ergste geval is er geen authenticatie nodig.
User Interaction (UI)	None	Geen interactie met andere gebruikers nodig.
Confidentiality Impact (VC)	Low	Gehashte wachtwoorden voor de users kunnen gelezen worden.
Integrity Impact (VI)	Low	De Windows-gebruiker kan de werking en de data van de applicatie beïnvloeden.
Availability Impact (VA)	High	De Windows-gebruiker kan de werking en de data van de applicatie beïnvloeden en dus ook onklaar maken.
Confidentiality Impact (SC)	None	Er is geen secundaire technische impact.
Integrity Impact (SI)	None	Er is geen secundaire technische impact.
Availability Impact (SA)	None	Er is geen secundaire technische impact.
Attack Vector (MAV)	Physical	Op verzoek van Kiesraad is de 'physical' MAV toegevoegd omdat zij stelt dat iedere gemeente aftekent op het gebruik van air-gapped systemen en netwerk waarin de software wordt gebruikt.
	Total score	Vector
	4.4	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N/MAV:P

Aanbeveling

- Installeer de applicatie in een beschermde folder, zoals Program Files. Draai het onder een service account met lage rechten, zoals 'LocalService' als een Windows service en zet de database ook in een beschermde folder, zoals ProgramData. Om te zorgen dat gebruikers met lagere rechten de applicatie nog kunnen op- of herstarten: zet in de installatiehandleiding dat de beheerder een account met beperkte rechten moet aanmaken en geef dit account uitvoerrechten op de service.
- Als bovenstaande niet kan: pas in elk geval de locatie aan naar 'localappdata', om te voorkomen dat de inhoud van de installatiefolder via het netwerk wordt gesynchroniseerd als de air-gap tijdelijk wegvalt.
- Pas de documentatie zo aan dat er geen twijfel meer mogelijk is dat er lokale accounts gebruikt moeten worden tijdens de installatie.

3.3.6 Geen limiet op het aantal inlogpogingen

Kwetsbaarheid-ID	KIESR-2602-A06
Eerder gerapporteerd als	A.2 - Rapportage_Pentest_Abacus_GR26 (Securance HackDefense)
Risico	Laag

Bron

- /account/login

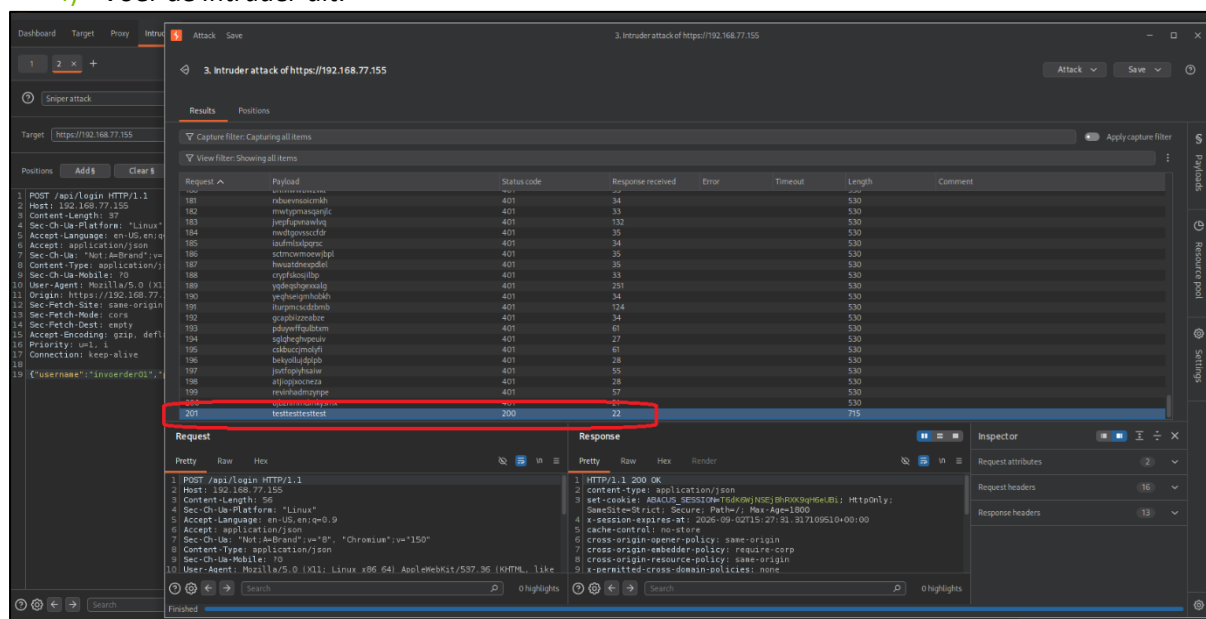
Beschrijving

De Abacus-applicatie voorziet in het gebruik van user accounts voor toegang tot verscheidene rollen of verkiezingsdata binnen de applicatie. Het is mogelijk om oneindig veel inlogpogingen te doen op deze applicatie.

Reproductie

Volg onderstaande reproductiestappen om deze kwetsbaarheid te verifiëren. Gebruik hierbij een proxy zoals Burp Suite. Deze moet eerst worden geconfigureerd om browserverkeer af te vangen.

- 1) Voer een inlogpoging uit met een bestaande username en foutief wachtwoord.
- 2) In BurpSuite, zend het *request* naar de *Intruder*.
- 3) Vul de *payload* voor het wachtwoord-veld met 200 entries met random karakters, en daarna met het juiste wachtwoord.
- 4) Voer de *Intruder* uit.



Figuur 8: Brute-force op wachtwoordveld.

Het resultaat laat 200 foutieve pogingen zien, waarna het juiste wachtwoord alsnog geaccepteerd wordt.

Impact: gemiddeld

Een aanval kan door middel van een brute-force aanval oneindig veel pogingen doen om een wachtwoord bij een bestaand account te achterhalen.

Kans: laag

Een gebruikersnaam is vereist om hierop een aanval uit te voeren, verder vereist het wachtwoordbeleid ten minste 13 karakters en is de software alleen benaderbaar vanuit het *air-gapped* netwerk.

Metrics	Scoring	Toelichting
Attack Vector (AV)	Network	Inlogpogingen worden uitgevoerd via het netwerk.
Attack Complexity (AC)	Low	Een brute-force aanval uitvoeren is triviaal.
Attack Requirements (AT)	None	
Privileges Required (PR)	Low	De aanvaller heeft geen additionele rechten nodig.
User Interaction (UI)	None	
Confidentiality Impact (VC)	None	
Integrity Impact (VI)	Low	Aangezien authenticatie incorrect wordt uitgevoerd, is de integriteit van het mechanisme niet langer gegarandeerd.
Availability Impact (VA)	None	
Confidentiality Impact (SC)	None	
Integrity Impact (SI)	None	
Availability Impact (SA)	None	
Attack Vector (MAV)	Physical	Op verzoek van Kiesraad is de 'physical' MAV toegevoegd omdat zij stelt dat iedere gemeente aftekent op het gebruik van air-gapped systemen en netwerk waarin de software wordt gebruikt.
	Total score	Vector
	2.4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/MAV:P

Aanbeveling

- Stel een korte wachttijd in (bijvoorbeeld 3 seconden) tussen opeenvolgende authenticatiepogingen, gebaseerd op het gebruikte account.
- Beperk het aantal authenticatiepogingen (bijvoorbeeld 60 per minuut) op basis van het IP-adres waarvan de pogingen afkomstig zijn.
- Hanteer een sterk wachtwoordbeleid.
- Log alle authenticatiepogingen en neem aanvullende maatregelen wanneer een brute-forceaanval wordt gedetecteerd.
- Implementeer tweefactorauthenticatie om de impact van gecompromitteerde wachtwoorden te beperken.

3.3.7 Geen restricties op namen van gebruikers

Kwetsbaarheid-ID	KIESR-2602-A07
Eerder gerapporteerd als	A.3 - Rapportage_Pentest_Abacus_GR26 (Securance HackDefense)
Risico	Laag

Bron

- Abacus-applicatie

Beschrijving

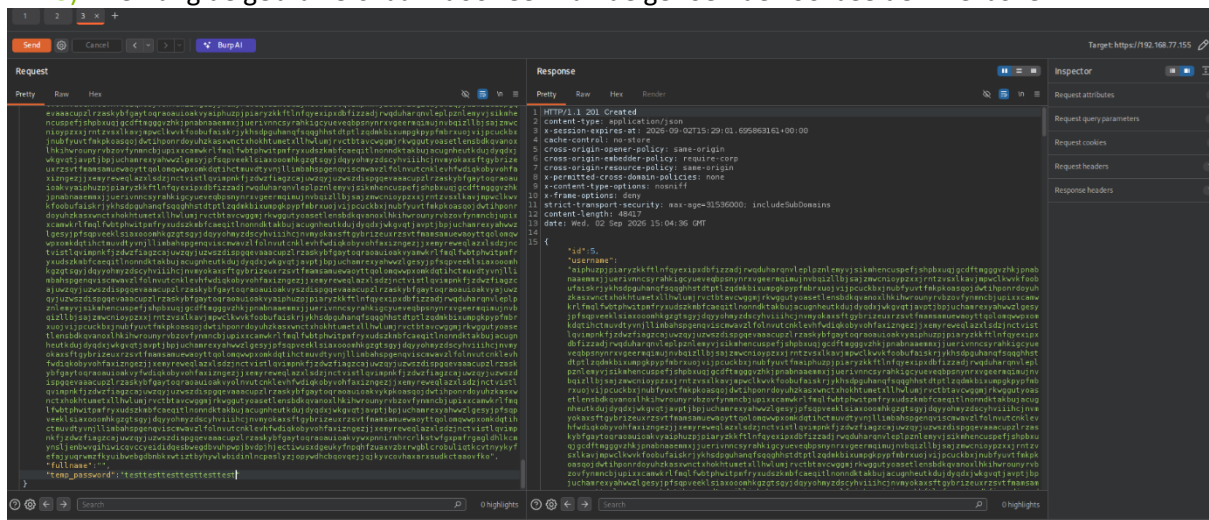
De Abacus-applicatie voorziet in het gebruik van user accounts voor toegang tot verscheidene rollen of verkiezingsdata binnen de applicatie. Het is mogelijk om zonder sluitende restricties gebruikersnamen in te stellen voor deze accounts. Het is bijvoorbeeld mogelijk om gebruikersnamen in te stellen met:

- een lege string
- een *newline* karakter
- meer dan 48000 willekeurige karakters.

Reproductie

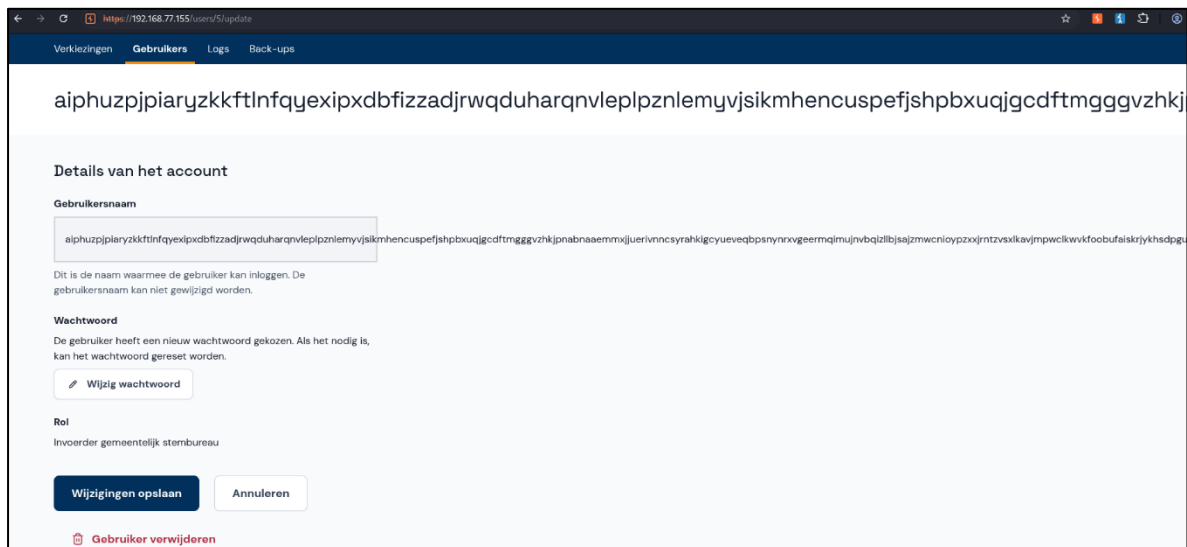
Volg onderstaande reproductiestappen om deze kwetsbaarheid te verifiëren. Gebruik hierbij een proxy zoals Burp Suite. Deze moet eerst worden geconfigureerd om browserverkeer af te vangen.

- 1) Log in de applicatie in.
- 2) Maak een nieuwe gebruiker aan en vang het *request* af in Burp Suite proxy.
- 3) Vervang de gebruikersnaam door een van de genoemde voorbeelden hierboven.



Figuur 9: Aangepast request om gebruikersnaam met 4800+ karakters aan te maken.

Het *request* wordt geaccepteerd met een “201 Created” en de user is aangemaakt.



Figuur 10: Gebruiker met lange gebruikersnaam is zichtbaar als valide account.

Impact: laag

Het kunnen aanmaken van gebruikersnamen met enorm veel karakters of bijvoorbeeld leeg, heeft geen directe impact op de security van de applicatie. De applicatie zou langzamer kunnen gaan werken door grotere hoeveelheden data te moeten verwerken.

Kans: laag

Alleen accounts met rechten om gebruikers aan te maken hebben de mogelijkheid om deze kwetsbaarheid uit te buiten.

CVSS 4.0 score

Metrics	Scoring	Toelichting
Attack Vector (AV)	Network	Gebruikersaccounts worden aangemaakt via de webapplicatie.
Attack Complexity (AC)	Low	Een gebruikersnaam voorzien van afwijkende of veel karakters is gemakkelijk uit te voeren.
Attack Requirements (AT)	None	
Privileges Required (PR)	Low	De aanvaller heeft geen additionele rechten nodig.
User Interaction (UI)	None	
Confidentiality Impact (VC)	None	
Integrity Impact (VI)	None	
Availability Impact (VA)	Low	De applicatie kan mogelijk minder goed gebruikt worden of langzamer reageren door grotere hoeveelheden data.
Confidentiality Impact (SC)	None	
Integrity Impact (SI)	None	
Availability Impact (SA)	None	
Attack Vector (MAV)	Physical	Op verzoek van Kiesraad is de 'physical' MAV toegevoegd omdat zij stelt dat iedere gemeente aftekent op het gebruik van air-gapped systemen en netwerk waarin de software wordt gebruikt.
	Total score	Vector

Metrics	Scoring	Toelichting
	2.4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/MAV:P

Aanbeveling

- Beperk de karakterset die in een gebruikersnaam kunnen voorkomen tot de relevante letters en leestekens.
- Beperk de lengte tot een redelijke lengte die voor iedereen genoeg is, maar geen technische problemen kan veroorzaken, zoals 100 of 200 karakters.

3.3.8 Achterhalen van gebruikersnamen mogelijk met time-base enumeratie

Kwetsbaarheid-ID	KIESR-2602-A08
Eerder gerapporteerd als	A.5 - Rapportage_Pentest_Abacus_GR26 (Securance HackDefense)
Risico	Laag

Bron

- /account/login

Beschrijving

De Abacus-applicatie voorziet in het gebruik van user accounts voor toegang tot verscheidene rollen of verkiezingsdata binnen de applicatie. Het is mogelijk om te achterhalen welke gebruikersnamen valide zijn op het system. De applicatie reageert langzamer op het controleren op foutieve inlogpogingen met accounts waar een correcte username gebruikt wordt dan bij accounts waar dat niet het geval is.

Reproductie

Volg onderstaande reproductiestappen om deze kwetsbaarheid te verifiëren. Gebruik hierbij een proxy zoals Burp Suite. Deze moet eerst worden geconfigureerd om browserverkeer af te vangen.

- 1) Voer een inlogpoging uit met een niet-bestaande username en wachtwoord.
- 2) In BurpSuite, zend het *request* naar de *Intruder*.
- 3) Vul de *payload* voor het username-veld met een aantal entries met willekeurige karakters, en daarna met een bestaande username.
- 4) Voer de *Intruder* uit.

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
43	invoerder00	401	4			530	
44	invoerder76	401	2			530	
45	invoerder68	401	4			530	
46	invoerder93	401	4			530	
47	invoerder28	401	3			530	
48	invoerder50	401	4			530	
49	invoerder63	401	3			530	
50	invoerder39	401	5			530	
51	invoerder82	401	2			530	
52	invoerder65	401	1			530	
53	invoerder20	401	3			530	
54	invoerder85	401	5			530	
55	invoerder16	401	2			530	
56	invoerder38	401	2			530	
57	invoerder33	401	2			530	
58	invoerder41	401	1			530	
59	invoerder43	401	1			530	
60	invoerder18	401	1			530	
61	invoerder88	401	2			530	
62	invoerder36	401	2			530	
63	invoerder01	401	32			530	
64	invoerder02	401	5			530	
65	invoerder97	401	7			530	
66	invoerder48	401	4			530	
67	invoerder31	401	4			530	
68	invoerder54	401	4			530	
69	invoerder30	401	4			530	
70	invoerder89	401	3			530	
71	invoerder71	401	3			530	
72	invoerder26	401	2			530	
73	invoerder22	401	7			530	
74	invoerder87	401	3			530	
75	invoerder27	401	2			530	

Figuur 11: Verschil in responsetijd bevestigt bestaan van gebruikersaccount.

De verschillen in *response*-tijd laten zien welke users bestaan op het systeem, en welke niet.

Impact: laag

De usernames worden specifiek voor de applicatie aangemaakt en zijn niet direct gekoppeld aan authenticatie elders. Deze kwetsbaarheid geeft inzicht in welke users er bestaan binnen de applicatie, waarna er een brute-force password aanval kan worden gedaan.

Kans: laag

De software is alleen benaderbaar vanuit het *air-gapped* netwerk.

Metrics	Scoring	Toelichting
Attack Vector (AV)	Network	Een inlogpoging wordt via het netwerk uitgevoerd.
Attack Complexity (AC)	Low	Het is triviaal om een inlogpoging uit te voeren.
Attack Requirements (AT)	None	Er zijn geen verdere vereisten voor deze aanval.
Privileges Required (PR)	None	Er zijn geen rechten nodig.
User Interaction (UI)	None	
Confidentiality Impact (VC)	None	Het is mogelijk om te bevestigen welke gebruikersnamen op het systeem bekend zijn.
Integrity Impact (VI)	None	
Availability Impact (VA)	None	
Confidentiality Impact (SC)	None	
Integrity Impact (SI)	None	
Availability Impact (SA)	None	
Attack Vector (MAV)	Physical	Op verzoek van Kiesraad is de 'physical' MAV toegevoegd omdat zij stelt dat iedere gemeente aftekent op het gebruik van air-gapped systemen en netwerk waarin de software wordt gebruikt.
	Total score	Vector
	2.4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/MAV:P

Aanbeveling

Zorg dat de reactietijd van elke inlogpoging gelijkwaardig is of voeg overal willekeurig vertraging toe om te zorgen dat er geen patroon zichtbaar is. Dit kan bijvoorbeeld door een uniforme authenticatieflow te implementeren: volg, na controle of een user wel of niet bestaat, de rest van de applicatielogica met een dummy hash. Wachtwoordchecks nemen dan evenveel tijd in beslag.

3.3.9 Air-gap-detectie vereist geen “no route to host”

Kwetsbaarheid-ID	KIESR-2602-A09
Eerder gerapporteerd als	A.7 - Rapportage_Pentest_Abacus_GR26 (Securance HackDefense)
Risico	Laag

Bron

- backend/src/api/middleware/airgap/detect.rs

Beschrijving

De Kiesraad vereist dat Abacus wordt uitgevoerd binnen een *air-gapped* netwerk. Dit betekent dat er geen internettoegang moet zijn. Als extra controle wordt hiertoe een melding getoond aan de gebruiker wanneer er wel internettoegang is gedetecteerd. De applicatie zal dan ook weigeren een loginscherm te tonen totdat er niet langer internettoegang is.

Om deze controle uit te voeren probeert Abacus te verbinden naar een aantal IP adressen. Wanneer dit succesvol is, concludeert de applicatie dat er internettoegang is. Als ergens op het netwerk de verbinding naar deze specifieke IP adressen wordt gefilterd, terwijl er verder volledige internettoegang is, concludeert de applicatie onterecht dat de *air-gap* correct werkt.

De Kiesraad geeft aan dat deze controle een dienst is om internettoegang welke onbewust aanwezig is te detecteren en niet bedoeld is om internet toegang ten alle tijden te voorkomen.

Reproductie

De code van de *air-gap*-detectie laat zien dat wanneer er een verbinding wordt gemaakt met een van de IP adressen de uitkomst *true* is. Zo niet, dan is het resultaat *false*. Als de verbinding niet gemaakt kan worden, bijvoorbeeld omdat deze IP adressen specifiek geblokkeerd worden, dan blijft het resultaat *true*.

```
// attempt to connect to known IP addresses over TCP
for ip in all_ip_addresses {
    set.spawn(async move {
        match timeout(
            CONNECT_TIMEOUT,
            tokio::net::TcpStream::connect((ip, SECURE_PORT)),
        )
        .await
        {
            Ok(Ok(_)) => {
                warn!("TCP connection to IP address {ip} successful");
                true
            }
            _ => false,
        }
    });
}
```

Impact: laag

Een onvolledige controle kan een vals beeld geven van de veiligheid van de situatie.

Kans: laag

De *air-gap*-detectie is een dienst om onbewust aanwezige internettoegang te detecteren. Gebruikers implementeren in principe een *air-gapped* netwerk.

CVSS 4.0 score

Metrics	Scoring	Toelichting
Attack Vector (AV)	Network	Internettoegang gaat via het netwerk.
Attack Complexity (AC)	Low	Het mogelijk ontbreken van een melding terwijl er wel internettoegang is, is mogelijk.
Attack Requirements (AT)	None	

Metrics	Scoring	Toelichting
Privileges Required (PR)	None	
User Interaction (UI)	None	
Confidentiality Impact (VC)	Low	Internettoegang kan gebruikt worden om data weg te sluizen of een aanvaller toegang te geven tot het netwerk.
Integrity Impact (VI)	None	
Availability Impact (VA)	None	
Confidentiality Impact (SC)	None	
Integrity Impact (SI)	None	
Availability Impact (SA)	None	
Attack Vector (MAV)	Physical	Op verzoek van Kiesraad is de 'physical' MAV toegevoegd omdat zij stelt dat iedere gemeente aftekent op het gebruik van air-gapped systemen en netwerk waarin de software wordt gebruikt.
	Total score	Vector
	2.4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/MAV:P

Aanbeveling

Verscherp controles op internettoegang door controle uit te voeren op de reden van het falen van een verbinding. Een 'no route to host' foutmelding zou een verbetering zijn ten opzichte van het alleen controleren of een verbinding gemaakt kan worden.

3.3.10 Voorspelbare hash-controle

Kwetsbaarheid-ID	KIESR-2602-A10
Eerder gerapporteerd als	A.9 - Rapportage_Pentest_Abacus_GR26 (Securance HackDefense)
Risico	Laag

Bron

- 'backend/src/eml/hash.rs'

Beschrijving

Bij het uploaden van een vierkiezingsdefinitie en kandidatenlijst moet de beheerder een stuk van de *hash* van het bestand invoeren. Deze *hash* is van tevoren aan de beheerder aangeleverd, samen met de bestanden. Door een deel van de *hash* in te laten voeren bewijst de beheerder dat het correcte bestand is geüpload. Deze controle dient om te voorkomen dat een beheer per ongeluk een verkeerd bestand uploadt.

De manier waarop de applicatie deze controle uitvoert kan echter gemanipuleerd worden. De applicatie deelt de *hash* in 16 stukjes en kiest een willekeurige waarde van de eerste 8 en de laatste 7.

- De *SmallRng* functie die daarvoor gebruikt wordt is niet geschikt omdat deze niet echt willekeurig is.
- De applicatie accepteert extra data aan het eind van de EML-bestanden, terwijl de EML data die het importeert hetzelfde is. Dit betekent dat een EML met dezelfde betekenis verschillende *hash*-waarden kan hebben.
- De totale set van $7 * 8$ mogelijkheden is erg klein. Als iemand van tevoren de EML-bestanden in handen krijgt kan in een paar uur met een brute-force aanpak een aangepaste EML gemaakt worden waarbij dezelfde 2 blokken van de *hash* toevallig dezelfde waarde hebben.

Reproductie

Inspecteer de *RedactedEmlHash* functie in *backend/src/eml/hash.rs*.

- Op regel 75 wordt de *SmallRng* struct gemaakt op basis van hash van het ingevoerde EML-bestand.
- Op regels 77 & 78 wordt de *random_range* functie vervolgens gebruikt om uit de eerste en de tweede helft een willekeurig block te kiezen.

```
abacus-1.1.0 > backend > src > eml > hash.rs
70
71 impl RedactedEmlHash {
72     fn random_chunk_indexes(digest: [u8; 32]) -> [usize; 2] {
73         use rand::{RngExt, SeedableRng};
74
75         let mut rng = SmallRng::from_seed(digest);
76         [
77             rng.random_range(0..CHUNK_COUNT / 2),
78             rng.random_range((CHUNK_COUNT / 2) + 1..CHUNK_COUNT),
79         ]
80     }
81 }
82
```

Figuur 12: selectie van de secties die de gebruiker moet invoeren.

Impact: gemiddeld

Er kan van elk geldig EML-bestand een kwaadaardige variant gemaakt worden die succesvol door dezelfde validatiefunctie komt. De beheerder kan wel zien op het scherm dat de rest van de *hash* niet klopt.

Kans: laag

Iemand moet van tevoren toegang hebben tot de EML-bestanden en deze op de USB-stick zetten. Om de data in te voeren is een beheeraccount nodig.

CVSS 4.0 score

Metrics	Scoring	Toelichting
Attack Vector (AV)	Network	Toegang gaat via het netwerk.
Attack Complexity (AC)	Low	Blocks die op de juiste plek kloppen kunnen betrouwbaar binnen een paar uur gemaakt worden.
Attack Requirements (AT)	None	Een aanvaller moet van tevoren de USB stick van de beheerder hebben kunnen compromitteren, of al eerder in het proces de bestanden aan hebben kunnen passen.
Privileges Required (PR)	None	De aanvaller heeft geen rechten nodig.
User Interaction (UI)	Passive	De beheerder moet het bestand importeren, maar dat is onderdeel van diens taak en gebeurt dus vanzelf.
Confidentiality Impact (VC)	None	
Integrity Impact (VI)	Low	De inhoud van de EML kan veranderd worden.
Availability Impact (VA)	None	
Confidentiality Impact (SC)	None	
Integrity Impact (SI)	None	
Availability Impact (SA)	None	
Attack Vector (MAV)	Physical	Op verzoek van Kiesraad is de 'physical' MAV toegevoegd omdat zij stelt dat iedere gemeente aftekent op het gebruik van air-gapped systemen en netwerk waarin de software wordt gebruikt.
	Total score	Vector
	1.0	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/MAV:P

Aanbeveling

- Keur een EML-bestand af als er data buiten het XML-document in het bestand staat.
- Gebruik een cryptografisch veilige *Random Number Generator* (RNG) en laat deze 2 willekeurige *blocks* uit de hele set van 16 selecteren.
- Voeg een instructie voor de beheerder toe om ook op het oog de rest van de *hash* te controleren.