

Toelichting pentest Abacus

De pentest van Abacus voor de herindelingsverkiezing 2026 Hilversum-Wijdemeren is uitgevoerd door Resillion. De pentest is een onafhankelijk onderzoek, waar de onderzoekers de ruimte hebben om hun eigen bevindingen terug te koppelen aan de Kiesraad.

Dit document geeft toelichting bij de vraag die is gesteld aan de onderzoekers en geeft een overzicht van de bevindingen en wat de Kiesraad ermee doet. Met dit document wordt invulling gegeven aan het streven direct bij publicatie meer informatie te delen.

Waarom deze pentest?

De uitslagprogrammatuur wordt voor elke verkiezing getest. De pentest richt zich specifiek op de beveiligingsaspecten van de uitslagprogrammatuur. In een apart onderzoek wordt getoetst of de programmatuur aan de wettelijke kaders voldoet.

Waar kan ik meer informatie vinden over de pentesten van Abacus?

Alle onderzoeken naar Abacus worden gepubliceerd op de website van de [Kiesraad](#). Voor de volledigheid zijn deze onderzoeken ook beschikbaar op [de documentatiepagina van Abacus](#) op GitHub, waar ook aanvullende context te vinden is over hoe we deze onderzoeken doen.

Hoe werken pentesten bij de Kiesraad?

Voor elke verkiezing wordt de uitslagprogrammatuur gepentest en getoetst aan de wettelijke kaders. Pentesten worden gecoördineerd door de CISO van de Kiesraad. De pentest wordt uitgevoerd door een van de organisaties die deelneemt aan de raamovereenkomst. Deze organisaties rouleren zodat waar mogelijk verschillende pentesters naar de uitslagprogrammatuur kijken.

Welke vraag is gesteld?

De vraag bestaat uit het voorgeschreven kader, de testdoelen, de scope en enkele aanwijzingen voor de rapportage en specifieke achtergrondinformatie:

Kader

- De pentest vindt hoofdzakelijk handmatig plaats. Daarbij mag gebruik worden gemaakt van geautomatiseerde tooling. De test dient hierbij een aanval van een kwaadwillende actor zo goed mogelijk te simuleren.

- De test zal worden uitgevoerd op een eigen in te richten netwerk. Denk hierbij aan een server, switch en clients.
- De Kiesraad zorgt voor de software en bijbehorende metadata/verkiezingsdefinitie.

Testdoelen

- In hoeverre is de software voldoende veilig om te gebruiken voor het doel (betrouwbare uitslag verkiezing)?
- In hoeverre is de installer vrij van plain text credentials of andere informatie waarvan het niet wenselijk is dat deze bekend raken?
- In hoeverre bevat de installer andere ongewenste informatie/data (malware bijvoorbeeld)?

In scope

Nadrukkelijk in scope zijn:

- DoS aanval (niet te verwarren met DDoS. Als het mogelijk is een DoS aanval te doen van binnen het netwerk, waarbij alleen de Kiesraad geraakt wordt, dan willen we dat weten).
- Brute forcing, password spraying en alle andere relevante toegangsaanvallen.
- XSS.
- SQL injectie.
- Misbruik van bekende kwetsbaarheden in gebruikte software.
- Misbruik van niet algemeen bekende kwetsbaarheden in gebruikte software (bijvoorbeeld zelf ontdekt tijdens de test).
- Nessus scan.
- Handmatig zoeken naar mogelijke kwetsbaarheden en de mogelijkheid hier misbruik van te maken.
- Gebruik van AI om naar de sourcecode te kijken en de output als bijlage mee te laten leveren.
- TLS, de correcte werking en implementatie van TLS (in de context van een lokaal, airgapped netwerk).

Verder alle andere relevante technieken en tooling welke voldoet aan de rest van de eisen uit dit document. Andere websites van de Kiesraad mogen worden geraadpleegd ter ondersteuning van eventueel advies.

Out of scope

- Elke vorm van red teaming.
- Elke vorm van social engineering.
- Alle tests welke de productieomgeving blijvend kunnen beschadigen of kwetsbaar kunnen maken voor aanvallen (blijvende backdoors inbouwen bijvoorbeeld).
- Infrastructuur anders dan vooraf uitdrukkelijk met toestemming besproken.
- Het afdwingen van een langer/complex wachtwoord.

Achtergrondinformatie

Hieronder geven we meer context bij bepaalde punten die out of scope zijn geplaatst:

Afdwingen langer/complexer wachtwoord:

Wachtwoorden in Abacus worden gebruikt voor rollenscheiding. Het is geen beveiligingsmaatregel. Beveiliging gebeurt op besturingssysteem-niveau.

Rapportage

In het rapport moet aan de CVSS *Base Score* een *Environmental Score* toegevoegd worden door een *Modified Attack Vector* op te nemen met de waarde P (*Physical*). Dit, omdat alle gemeenten de opdracht krijgen (en hier ook voor moeten tekenen) dat het netwerk air gapped is uitgevoerd. Dit dient ook om de scores in lijn te houden met voorgaande rapportages.

Tabel met bevindingen

Onderstaande tabel geeft een overzicht van de bevindingen uit de pentest van Resillion, voorzien van een reactie van de Kiesraad.

Bevindingen	Risico	Reactie	Uitleg	Issue GitHub
3.3.1 Invoerders kunnen willekeurige voortgangsperscentages instellen.	Informatief	Fix (deels) voor PS/WS	We gaan zorgen dat het niet mogelijk is om boven de 100% in te voeren om verwarring te voorkomen. Een andere aanpassing kost relatief veel ontwikkelcapaciteit ten opzichte van het risico dat ermee afgedekt zou worden.	Kiesraad / abacus#4010 (1.2)
3.3.2 Geen controle of stembureaus bij verkiezingen horen.	Laag	Onderzoek	Als niet de normale route door de applicatie wordt gevolgd, ontbreekt er een waarschuwing. We overwegen om dit gelijk te trekken.	Kiesraad / abacus#3895 (1.2)
3.3.3 Archief met uitslag definitieve zitting kan verkeerde	Informatief	Fix voor herindeling	Wordt opgelost voor de herindelingsverkiezing Hilversum-Wijdemeren 2026.	Kiesraad / abacus#3924 (1.1,

Bevindingen	Risico	Reactie	Uitleg	Issue GitHub
bestanden bevatten.				opgelost in 1.1.1)
3.3.4 Linux service niet optimaal gehard.	Informatief	Fix voor PS/WS	Bij de herindelingsverkiezing Hilversum-Wijdmeren 2026 wordt geen Linux gebruikt.	Kiesraad /abacus #4011 (1.2)
3.3.5 Abacus voor Windows installeert in persoonlijke AD folder.	Laag	Fix voor herindeling	Wordt opgelost voor herindelingsverkiezing. De suggestie om een Windows service toe te passen doen we in een latere versie.	Kiesraad /abacus #3925 (1.1, opgelost in 1.1.1) Kiesraad /abacus #3237 (1.2)
3.3.6 Geen limiet op het aantal inlogpogingen.	Laag	Onderzoek voor PS/WS	Onderzoek welke oplossingen zouden kunnen werken die niet voor andere problemen zoals een denial of service zorgen.	Kiesraad /abacus #4012 (1.2)
3.3.7 Geen restricties op namen van gebruikers.	Laag	Onderzoek voor PS/WS	We gaan onderzoeken of een maximale lengte een optie is en het beperken tot alfanumerieke karakters.	Kiesraad /abacus #4013 (1.2)

Bevindingen	Risico	Reactie	Uitleg	Issue GitHub
3.3.8 Achterhalen van gebruikersnamen mogelijk met time-base enumeratie.	Laag	Onderzoek voor PS/WS	We gaan onderzoeken welke mogelijkheden hiervoor kunnen werken.	Kiesraad /abacus #4014 (1.2)
3.3.9 Airgap-detectie vereist geen "no route to host".	Laag	Onderzoek voor PS/WS	We gaan onderzoeken welke mogelijkheden hiervoor kunnen werken.	Kiesraad /abacus #4015 (1.2)
3.3.10 Voorspelbare hash-controle.	Laag	Onderzoek voor PS/WS	We gaan onderzoeken welke mogelijkheden hiervoor kunnen werken.	Kiesraad /abacus #4016 (1.2)