Security advies Abacus

toelichting en omgang met de aanbevelingen

Veritas heeft op verzoek van de Kiesraad een onderzoek gedaan naar de beveiligingsaspecten van Abacus.

De Kiesraad is de onderzoekers zeer erkentelijk voor hun werk en het opgeleverde rapport. De suggesties uit het rapport kunnen we grotendeels overnemen, waarmee het rapport een goede bijdrage levert aan de kwaliteit van de software.

Conclusie

De belangrijkste conclusie uit het rapport is dat Abacus over het geheel genomen 'robuust' is en er geen hoge of kritieke risico's zijn gevonden:

Tijdens het onderzoek zijn in het ontwerp of de (kern-)broncode van de ontwikkelversie van Abacus zelf geen ernstige tekortkomingen geconstateerd. Bij een steekproefsgewijze controle van invoervalidatie, autorisatiecontroles en veelvoorkomende softwarekwetsbaarheden bleek Abacus robuust.

Het antwoord op de vraag of er 'laaghangend fruit' is aangetroffen luidt dus ontkennend: er zijn geen kwetsbaarheden geïdentificeerd die, binnen de specifieke context waarin Abacus wordt gebruikt, een hoog of kritiek risico opleveren.

De onderzoekers hebben aandachtspunten benoemd waarmee we Abacus kunnen verbeteren. De aandachtspunten zijn grotendeels interessante suggesties, waar we deels al mee bezig zijn of bewuste afwegingen over gemaakt hebben. Dit bespreken we hieronder.

Aandachtspunten

De aandachtspunten zijn ook te vinden in het rapport. Per aandachtspunt is een korte uitleg opgenomen.

Uitleg aandachtspunten

Aandachtspunt	Onderwerp	Uitleg
1	Overweeg technisch te controleren dat de server niet als invoerstation wordt gebruikt.	De server is de plek waar Abacus op geïnstalleerd wordt. De laptops (clients) navigeren daarnaartoe over het air-gapped netwerk. De server wordt alleen gebruikt door beheerders. Het is niet nodig als invoerstation. Door het wel als invoerstation te gebruiken stel je het mogelijk onnodig bloot aan storingen/fouten/misbruik.
2	Pas identiteitsgebonden code-signing toe op binary's.	Door dit toe te passen voeg je een extra mogelijkheid toe voor gemeenten om zekerheid te krijgen dat zij een officiële versie van Abacus hebben en geen namaak/andere versie.
3	Voeg airgapdetectie toe aan de frontend.	Nu controleert Abacus alleen op internetverbinding aan de kant van de server. Dat is ook de plek waar de meest gevoelige onderdelen van Abacus staan. Veritas beveelt aan de controle ook op de laptops (clients/frontend) te doen.
4	Overweeg ICMP-test toe te voegen aan de airgapdetectie op de backend.	Nu controleert Abacus of er sprake is van een internetverbinding op verschillende netwerklagen (netwerkverkeer is gelaagd). ICMP voegt daar een extra laag aan toe. Daarmee geeft het nóg meer zekerheid dat er geen internetverbinding is.
5	Zorg dat de releaseversie van Abacus geen test-secrets bevat in broncode en/of binary builds.	In de ontwikkelversie van Abacus staat informatie die bedoeld is om het testen te vereenvoudigen. Als deze ook in de versie van Abacus staan die we gaan gebruiken, kan dit tot misverstanden leiden over de veiligheid.
6	Overweeg 'reproducable builds' van Abacus als punt op de horizon voor de lange termijn.	Met reproducable builds kan eenieder vanuit de broncode van Abacus de software op het allerlaagste computerniveau zelf identiek maken aan de Abacus die in gebruik is. Dit zorgt voor extra transparantie, maar is om verschillende redenen complex om te realiseren.
7	Supply chain: dreiging van compromittering van een dependency-ontwikkelaar.	Abacus leunt voor sommige onderdelen op software die is gemaakt door anderen ('dependency's'). Veritas waarschuwt voor het risico dat een ontwikkelaar hiervan opzettelijk een kwetsbaarheid kan inbouwen waarmee Abacus niet langer betrouwbaar is. Dit gebeurt dan buiten het directe zicht van de ontwikkelaars om.
8	Twee transitieve dependency's van backend hebben status 'unmaintained'.	Veritas beschrijft dat er twee van de hierboven beschreven dependency's zijn waarvan al is aangegeven dat deze niet langer worden voorzien van (beveiligings)updates.
9	Suggesties voor ondertekenmechanisme uitslagbestanden.	Veritas doet suggesties voor het toepassen van afzenderverificatie (vergelijkbaar met hoe het nu in OSV werkt met de sleutels en het ondertekenen van de EML bestanden).

10	Aanbevelingen inzake onderscheppen netwerkverkeer.	Netwerkverkeer van Abacus is niet versleuteld tussen de laptops (clients) en de server. Daarmee zou iemand die fysiek bij het Abacus netwerk kan, zien en mogelijk ook kunnen manipuleren wat er tussen de laptops (clients) en de server gebeurt. Veritas doet hier aanbevelingen over.
11	Adviezen met betrekking tot wachtwoordbeleid.	Veritas doet een aantal aanbevelingen omtrent het wachtwoordbeleid.

Reactie aandachtspunten

Aandachtspunt	Onderwerp	Overnemen j/n	Toelichting
1	Overweeg technisch te controleren dat de server niet als invoerstation wordt gebruikt.	X	Wij zien hier meerwaarde in en we gaan onderzoeken of dit mogelijk/haalbaar is.
2	Pas identiteitsgebonden code-signing toe op binary's.	J	Hier werken we al aan.
3	Voeg airgapdetectie toe aan de frontend.	J	Wij zien hier meerwaarde in en nemen het over. We zetten dit op de to-do lijst.
4	Overweeg ICMP-test toe te voegen aan de airgapdetectie op de backend.	J	We zien hier meerwaarde in en we gaan onderzoeken of dit mogelijk/haalbaar is. We zetten deze op de to-do lijst
5	Zorg dat de releaseversie van Abacus geen test-secrets bevat in broncode en/of binary builds.	J	Vanzelfsprekend. De tests zijn geen onderdeel van de productierelease.
6	Overweeg 'reproducable builds' van Abacus als punt op de horizon voor de lange termijn.	J	Wij zien hier meerwaarde in. Op dit moment is het met de technische randvoorwaarden nog niet mogelijk om dit toe te passen. Het is zeker een wens voor de lange termijn.
7	Supply chain: dreiging van compromittering van een dependency-ontwikkelaar.	X	De aanbevelingen hebben op beveiligingsgebied ook nadelen. Bijvoorbeeld doordat beveiligingsupdates niet meer meegenomen kunnen worden door een bevriezingsperiode.
8	Twee transitieve dependency's van backend hebben status 'unmaintained'.		In de praktijk is er bij 1 dependency sprake van de status 'unmaintained'. Dit is een stabiele situatie, bij wijzigingen valt dit direct op. Nadere toelichting is hieronder opgenomen.

9	Suggesties voor ondertekenmechanisme uitslagbestanden.	J	We werken momenteel aan een proof of concept naar een eerder gemaakt ontwerp.
10	Aanbevelingen inzake onderscheppen netwerkverkeer.	N	Het beveiligingsrisico is bij de risicoanalyse ingeschat als klein door de omliggende technische en procedurele maatregelen. Het beperken van dit risico met technische maatregelen leidt tot een verhoogde beheerlast die in de afweging niet opweegt tegen het risico. Nadere toelichting is hieronder opgenomen.
11	Adviezen met betrekking tot wachtwoordbeleid.	X	Wachtwoorden in Abacus zijn voornamelijk bedoeld om rollen te kunnen scheiden en niet als beveiligingsmaatregel tegen aanvallers. Daarom wordt de suggestie om met een blocklist te werken niet overgenomen.

Nadere toelichting

De meeste suggesties van de onderzoekers worden in dank aanvaard en overgenomen. Deels moeten ze worden onderzocht, deels kunnen ze op korte termijn worden toegepast. In drie gevallen hebben we nadere toelichting opgenomen:

Onderscheppen van het netwerkverkeer

Er wordt aanbevolen om de mogelijkheid te beperken dat het verkeer binnen het airgapped netwerk wordt onderschept. Bij de risicoanalyse is dit risico als klein ingeschat.. Een technische afvanging van dit risico zou veel extra handelingen van de gebruikers opleveren. De afweging tussen de omvang van het risico en de benodigde maatregelen en extra handelingen van de gebruikers van Abacus leidt tot de conclusie dat het risico klein genoeg is en er voldoende omliggende maatregelen zijn om het te accepteren.

Om Abacus te kunnen gebruiken wordt in iedere gemeente een apart lokaal netwerk opgezet, met de Abacus server en de invoerstations. Dit netwerk heeft verder geen verbinding, met andere netwerken of het internet. Daarnaast zijn er procedurele eisen aan het gebruik van Abacus, zoals beveiliging van de ruimte waarin de software wordt gebruikt, het controleprotocol optellingen waarmee de in- en output van Abacus handmatig worden vergeleken, de data-analyses van de Kiesraad en de publicatie van alle bestanden zodat eenieder de uitslagen kan controleren.

Het is een andere afweging dan eerder voor OSV en OSV2020 is gemaakt, waar de beheerder op elk werkstation in de browser een zelf aangemaakt certificaat installeert en vertrouwt. Dit is een handmatig proces dat veel tijd vraagt. In het licht van de inschaling van het risico is bij Abacus gekozen om dit niet te verplichten.

Het blijft een afweging tussen de uitvoeringslast en meerwaarde van de maatregel. Op het moment is echter de inschatting dat in het licht van de uitvoeringslast de huidige technische, beheers- en controlemaatregelen voldoende zijn om dit risico te mitigeren.

Dependencies

De suggesties van de onderzoekers bieden uitstekende aanknopingspunten om het testen en beoordelen van de gebruikte dependencies te verbeteren en worden in dank aanvaard. Een van de aandachtspunten lichten we nader toe:

Twee dependencies hebben de status 'unmaintained'. Een van de genoemde afhankelijkheden vormt zoals de onderzoekers aangeven geen relevant risico, omdat de maker hiervan een bekende Rust developer is en van mening is dat er geen noodzaak is aan deze software nader te werken.

De andere afhankelijkheid zit in een stuk software dat Abacus gebruikt om pdfs te genereren, maar het specifieke onderdeel waarin de afhankelijkheid zit, heeft Abacus niet nodig. Je kunt de twee onderdelen echter niet los van elkaar in Abacus opnemen. De software is stabiel dus het risico schatten wij momenteel in als klein. In overleg met de ontwikkelaars van de software die de pdfs genereert wordt gekeken of het mogelijk is om hier wat aan te doen.

Wachtwoordbeleid

De onderzoekers suggereren een aantal maatregelen rondom het inloggen. Een deel van deze maatregelen zijn tijdens het onderzoek direct toegepast (zoals het loggen van mislukte inlogpogingen), de overige maatregelen worden voor de toekomst meegenomen.

Tijdens het gebruik van Abacus is het inloggen vooral een manier om rollenscheiding te bewerkstelligen, geen authenticatie in de klassieke zin. Dat maakt dat een aantal afwegingen rondom wachtwoorden anders uitvallen.

De suggestie om een blocklist op te nemen passen we nog niet toe. Aangezien de doelstelling van de gebruikersnaam en wachtwoord in Abacus vinden we het niet nodig om deze aanpassing toe te voegen.