Oplegger

Rapport pentest Vorderingenoverzicht Rijk

14-03-2024

Inhoudsopgave

Managementsamenvatting

In 2023 is een penetratietest uitgevoerd op (de demo-omgeving van) Vorderingenoverzicht Rijk. Dit document betreft een geanonimiseerde versie van het pentestrapport. Door het rapport te publiceren, laten we zien dat we transparant en open werken. Deze transparantie en openheid dragen bij aan veiligere software voor burgers en organisaties. Het rapport is deels geanonimiseerd, namen en aanverwante zaken zijn afgeschermd. Daarnaast voorzien we het rapport met deze oplegger van aanvullende informatie en context.

Bij de ontwikkeling van het VO Rijk passen we nadrukkelijk de principes van privacy en security by design toe. Dat is één van de redenen, dat we een de oplossing niet achteraf laten toetsen, maar al tijdens de ontwikkeling. Dit biedt als voordeel dat we al vroegtijdig richting en aannames kunnen meenemen in de test. Ook kunnen we bijsturen voordat de volledige implementatie heeft plaatsgevonden. Enkele paren extra ogen zorgen bij het team voor bewustzijn van aanwezige biases en risico's. Deze aanpak past goed bij onze transparante werkwijze.

Samenvatting van de analyse

Het ontwikkelteam had een substantieel aantal risico's reeds in beeld. Daarnaast heeft de pentest een aantal waardevolle nieuwe inzichten opgeleverd. Ook niet onbelangrijk: de resultaten geven ook de juiste basis om prioriteit te geven aan deze onderwerpen in de ontwikkeling van het VO Rijk. Productwaarde is namelijk leidend in de volgorde waarin onderwerpen worden opgepakt.

Belangrijkste actiepunten

Verbeteringen t.b.v. de bescherming van de gegevens op het apparaat van de gebruiker:

Bevinding	*Status*
Encryptie van gegevens op apparaat gebruiker	opgelost
Bescherming sleutelmateriaal: SE/TEE	onderhanden
Toegangscode: sluitsteen van bescherming gegevens op apparaat gebruiker	ontworpen, staat met hoge prioriteit op backlog

Verbeteringen t.b.v. het protocol:

Bevinding	*Status*
Revocation/expiration	opgelost
Certificate pinning	op backlog, lage prioriteit
Toepassen standaarden voor signing en encryptie	opgelost
Beschrijving standaarden en cryptografie	onderhanden

Actiepunten die raken aan UX:

Enkele van deze actiepunten, zoals jailbreak-bescherming, bescherming tegen schermopnames en time-out bescherming vergen meer dan enkel technische afweging. Deze punten vergen nader UX-onderzoek om samen met gebruikers de sweet spot te vinden waar (technische) bescherming en (praktische) gebruikersvriendelijkheid samenkomen. Overmatige technische bescherming kan er namelijk ook toe leiden dat gebruikers zich beperkt voelen en 'om de bescherming heen gaan werken' wat dan juist kan zorgen voor onveiligere situaties. Daarom onderzoeken we deze punten samen met gebruikers.

Overige actiepunten:

Van de overige bevindingen is een analyse gemaakt, en deze punten zijn opgelost waar nodig.

Vervolg van het traject

Het vervolg van dit traject laat zich als volgt schetsen:

- Activiteiten op onderhanden maatregelen/acties worden afgerond
- Acties/maatregelen die op de backlog staan worden met de juiste prioriteit opgepakt
- Voor het operationaliseren van het VO Rijk, zal opnieuw een pentest worden uitgevoerd, (mede) om de getroffen maatregelen te toetsen

Bevindingen, risico's en maatregelen

Deze paragraaf bevat een beknopte samenvatting van de in de pentest geïdentificeerde bevindingen, de risico-inschatting door team Vorderingenoverzicht Rijk, en de beoogde maatregelen plus actuele status.

L01 Er wordt gebruik gemaakt van een ongeldig certificaat met in de CN: Kubernetes Ingress Controller Fake Certificate.

Risico	Het gebruik van een ongeldig certificaat op het cluster kan het risico vergroten dat gebruikers ook andere ongeldige certificaten gaan vertrouwen, en dus dat een aanvaller zich kan voordoen als een van de deelnemers.
Analyse	Dit betreft alleen het default certificaat op het k8s cluster van de demo-omgeving. Er is geen direct risico voor de Demo omgeving (alle componenten hebben wel een geldig certificaat).
Maatregelen	Geen directe maatregelen (op productieclusters zal dit wel geregeld moeten zijn).
Status	Afgehandeld, inmiddels is de hele demo-omgeving verhuisd naar een nieuw cluster bij Digilab.

A01 Zorg dat onnodige endpoints worden verwijderd als het product in productie gebruikt gaat worden.

Risico	Onnodige endpoints kunnen door aanvallers misbruikt worden (groter aanvalsvlak).
Analyse	Dit betreft geen onnodige endpoints.
Maatregelen	Geen directe maatregelen. Deze endpoints zijn ook in productie nodig.
Status	Afgehandeld

L02 Het certificaat logboeksysteem van Letsencrypt stelt een aanvaller in staat om beheer interfaces te achterhalen

Risico	Aanvallers kunnen via het certificaatlogboek van Letsencrypt ook adressen verkrijgen van beheerinterfaces.
Analyse	Voor de demo-omgeving is bewust gekozen de beheeromgevingen ook publiek beschikbaar te maken voor demonstratiedoeleinden. In productie zullen beheeromgevingen niet publiek beschikbaar mogen zijn.
Maatregelen	Geen directe maatregelen. Deze componenten zijn niet standaard publiek beschikbaar, maar alleen als dat bij operatie geregeld wordt.
Status	Afgehandeld

A02 Wees ervan op de hoogte dat vorderingenoverzicht.app een registreerbaar domein is. Mogelijk kan deze gebruikt worden voor een phishing campagne of om misbruik te maken van deeplinks.

Risico	Een aanvaller kan het domein registreren en op die manier deeplinks naar de app stelen, of de app imiteren. Ook kan dit een risico zijn voor het gebruik van de naam Vorderingenoverzicht.
Analyse	Hoewel de naam Vorderingenoverzicht Rijk een werktitel is, is dit is een risico dat we direct willen mitigeren, en dat is makkelijk te regelen.
Maatregelen	Domein vorderingenoverzicht.app zelf registreren.
Status	Afgehandeld, domein is inmiddels in bezit van Team Vorderingenoverzicht Rijk.

M01 De app heeft geen iOS jailbreak detectie.

Risico	Wanneer de telefoon van de gebruiker gejailbreakt is, kan het zijn dat niet alle beveiligingsmaatregelen om de informatie op de telefoon te beschermen even effectief zijn als op niet-gejailbreakte apparaten.

Analyse	Het staat gebruikers vrij om zelf te kiezen om hun telefoon wel of niet te jailbreaken. Tegelijk willen we gebruikers ook informeren en helpen veilige keuzes te maken. Het kan namelijk dat gebruikers zich niet bewust zijn van de risico's van jailbreaken of dat zij niet op de hoogte zijn van het jailbreaken. Daarom is het verstandig om uiteindelijk de gebruiker wel te informeren over de risico's van jailbreaken, maar gebruik van de applicatie niet onmogelijk te maken.
Maatregelen	Jailbreakdetectie en het informeren van de gebruiker risico's toevoegen aan de backlog. Lage prioriteit. Vereist UX-onderzoek en technisch onderzoek.
Status	mogelijk later oppakken, nu lage prioriteit.

L03 De applicatie maakt geen gebruik van certificate pinning. Hierdoor kan verkeer van en naar de server onderschept wordt.

Risico	Het risico is dat gebruikers contact hebben met een andere partij dan zij denken, omdat een wederpartij weliswaar een geldig certificaat presenteert maar dit niet het certificaat is van de partij die is goedgekeurd voor deelname aan de het stelsel.
Analyse	Het mitigeren van dit risico is een belangrijk onderdeel van het protocol van Vorderingenoverzicht Rijk (Blauwe Knop Connect), en staat op de backlog.
Maatregelen	De stelselbeheerder het stelseldocument laten ondertekenen, het stelsel bevat vervolgens de sleutels van de deelnemende organisaties, en de app controleert deze sleutels tijdens het verbinden
Status	Op backlog

L04 De applicatie is niet beveiligd tegen het maken van schermopnames. Hierdoor is het eenvoudiger voor andere personen om schulden in te zien.

Risico	Het risico is dat gebruikers schermopnamen of screenshots maken van het vorderingenoverzicht en dat die beelden bij derde partijen belanden
Analyse	Schermopnames maken is ook een laagdrempelige manier voor mensen om hun eigen gegevens te gebruiken zoals zij willen. We willen dit nu niet verbieden maar meer gebruikersonderzoek doen hoe burgers de data willen gebruiken en in welke situaties zij schermopnamen willen kunnen maken. Als we weten wat gewenst gebruik is kunnen we een goed alternatief bieden, tot die tijd is verbieden ook een (groter) risico, omdat gebruikers dan onveiligere geitenpaadjes gaan gebruiken om toch voor elkaar te krijgen wat zij willen doen.
Maatregelen	Aanvullend gebruikersonderzoek doen over de manier waarop gebruikers hun gegevens willen gebruiken.
Status	Mogelijk later oppakken, nu lage prioriteit.

A03 Geen time-out vergrendeling van de applicatie.

Risico	Als de app ontgrendeld blijft nadat gebruikers deze hebben gebruikt, kan een aanvaller wellicht de app ook gebruiken als gebruikers hun apparaat even niet in de gaten houden.
Analyse	Het automatisch vergrendelen van de app na een bepaalde tijd is verstandig om door te voeren. Het moet niet irritant zijn voor gebruikers, anders gaan zij om de vergrendeling heen werken met geitenpaadjes die onveiliger zijn, maar dit is prima samen met gebruikers in gebruikersonderzoek te ontwerpen.
Maatregelen	Time-out functionaliteit ontwerpen samen met gebruikers en implementeren.
Status	Op backlog

M02 De applicatie maakt geen gebruik van een toegangscode/biometrische authenticatie. Hierdoor is het eenvoudiger voor andere personen om schulden in te zien.

Risico	Als de toegang tot de applicatie niet beveiligd is met een pincode, kan een aanvaller die toegang heeft tot de telefoon ook direct toegang krijgen tot de applicatie en de data die erin aanwezig is. Dit kan bijvoorbeeld gebeuren als mensen hun telefoon verliezen of tijdelijk in handen van een derde persoon geven.
Analyse	Het mitigeren van dit risico is een belangrijk onderdeel van het ontwerp van de Vorderingenoverzicht Rijk applicatie, en staat op de backlog. Het heeft echter pas waarde om dit punt op te pakken nadat we de encryptie van gegevens op het apparaat van de burger en het beschermen van de persoonlijke sleutels van de burger hebben geïmplementeerd (zie volgende punten). Daarom staat dit punt onder die punten op de backlog.

Maatregelen	Toegangscode/biometrie implementeren als toegangscontrole tot de app (vergelijkbaar met hoe bank-apps dit doen).
Status	Op backlog

L05 De private key wordt onversleuteld opgeslagen.

Risico	Wanneer de private key onversleuteld wordt opgeslagen, is het risico groter dat een aanvaller toegang verkrijgt tot de private key, en zich daarmee kan uitgeven voor de gebruiker.
Analyse	Het mitigeren van dit risico is een belangrijk onderdeel van het ontwerp van de Vorderingenoverzicht Rijk applicatie, en staat op de backlog met hoge prioriteit. Naar oordeel van Team Vorderingenoverzicht Rijk zou dit item ook wel gecategoriseerd kunnen worden als Middel (en M03 juist als Laag).
Maatregelen	De private key van de gebruiker opslaan en gebruiken in Secure Enclave (iOS) of TEE (Android). Op web de private key eveneens adequaat beveiligen of elk gebruik roteren.
Status	Onderhanden

M03 De private key voor het versleutelen van data wordt opgeslagen in de isar database file.

Risico	Wanneer de private key onversleuteld wordt opgeslagen, is het risico groter dat een aanvaller toegang verkrijgt tot de private key, en zich daarmee kan uitgeven voor de gebruiker. Omdat de private key in de onversleutelde database wordt opgeslagen is dit risico aanwezig.
Analyse	Het mitigeren van dit risico is een belangrijk onderdeel van het ontwerp van de Vorderingenoverzicht Rijk applicatie. De Vorderingenoverzicht Rijk applicatie gebruikt Isar als databasesysteem, en daarin wordt de database momenteel niet versleuteld opgeslagen. Deze functionaliteit was wel beschikbaar in Isar, maar is in de nieuwste versie van Isar niet meer beschikbaar. We moeten deze functionaliteit dus toevoegen of een andere databasetechnologie gebruiken (zie ook L06). Bovendien willen we de private key uiteindelijk sowieso niet meer opslaan in de database, maar in SE/TEE (zie L05).
Maatregelen	Zorgen dat alle gegevens altijd encrypted worden opgeslagen op het apparaat van de gebruiker (zie ook L06). Later (wanneer we L05 oplossen): de private key van de gebruiker opslaan en gebruiken in Secure Enclave (iOS) of TEE (Android).
Status	Afgehandeld, de Isar databasetechnologie is vervangen door een andere technologie, die wel encrypted storage ondersteunt. Punt L05 is onderhanden.

L06 De database bevat onversleutelde data.

Risico	Wanneer de data van de gebruiker (bijvoorbeeld gegevens over financiële verplichtingen) onversleuteld wordt opgeslagen, is het risico groter dat een aanvaller zich daar toegang toe verschaft. Omdat de data onversleutelde database wordt opgeslagen is dit risico aanwezig.
Analyse	Het mitigeren van dit risico is een belangrijk onderdeel van het ontwerp van de Vorderingenoverzicht Rijk applicatie. De Vorderingenoverzicht Rijk applicatie gebruikt Isar als databasesysteem, en daarin wordt de database momenteel niet versleuteld opgeslagen. Deze functionaliteit was wel beschikbaar in Isar, maar is in de nieuwste versie van Isar niet meer beschikbaar.
Maatregelen	Zorgen dat alle gegevens altijd encrypted worden opgeslagen op het apparaat van de gebruiker.
Status	Afgehandeld, de Isar databasetechnologie is vervangen door een andere technologie, die wel encrypted storage ondersteunt.

M04 Database met gevoelige gegevens wordt niet verwijderd bij het leegmaken van de app.

Risico	Wanneer de database file bij het leegmaken van de app niet wordt verwijderd, kunnen gegevens van de gebruiker geheel of gedeeltelijk achterblijven op het apparaat van de gebruiker, terwijl deze denkt dat de gegevens verwijderd zijn. Dat vergroot het risico dat de gegevens later toch nog toegankelijk zijn voor aanvallers.
Analyse	Het is belangrijk dit punt te mitigeren.
Maatregelen	Bij het leegmaken van de app ook alle databases legen en het databasebestand verwijderen/resetten.
Status	Afgehandeld

M05 Database met gevoelige gegevens bevindt zich in een map die mee wordt genomen in de back-ups.

Risico	Wanneer een database met gevoelige gegevens mee wordt genomen in automatische back-ups, komen deze gegevens ook terecht op de locatie die voor deze back-ups wordt gebruikt, bijvoorbeeld bij Apple of Google of op een eigen back-up-apparaat. Dat vergroot het risico dat deze gegevens elders belanden.
Analyse	Dat gegevens meegaan in een back-up is inderdaad een risico, maar het is aan gebruikers zelf of zij gegevens wel of niet willen back-uppen. Het niet hebben van back-ups is immers ook een risico waarvoor gebruikers zich wellicht willen beschermen. Desalniettemin is dit een goed punt om nader gebruikersonderzoek naar te doen en waar nodig aanvullende functionaliteit voor te implementeren.
Maatregelen	Aanvullend gebruikersonderzoek doen over de manier waarop gebruikers hun gegevens willen back-uppen. Eventueel aanvullende mogelijkheden bieden om back-ups aan of uit te zetten zodat gebruikers hier zelf over in controle zijn.
Status	Op backlog, mogelijk later oppakken, nu geen hoge prioriteit.

H01 De database waarin de onversleutelde private key en onversleutelde data over schulden van de gebruiker staan, bevindt zich in een map die mee wordt genomen in de back-ups. Daardoor kunnen ze op een PC belanden of in de iCloud back-updienst.

Risico	Wanneer de public key onversleuteld wordt opgeslagen (L05) in de databasefile (M03) die onversleuteld is (L06) en meegenomen wordt in back-ups (M05), dan is het risico zeer groot dat de private key van de gebruiker onvoldoende beschermd is. Deze kan dan op een PC of cloud-back-updienst belanden.
Analyse	Het mitigeren van dit risico is een belangrijk onderdeel van het ontwerp van de Vorderingenoverzicht Rijk applicatie. Het staat buiten kijf dat we de afzonderlijke punten die tot dit samengestelde punt leiden moeten mitigeren.
Maatregelen	De maatregelen zoals genoemd bij L05, M03, L06 uitvoeren.
Status	M03/L06 is afgehandeld, maar aangezien L05 onderhanden is, is dit punt ook nog onderhanden.

M06 RSA-implementatie maakt geen gebruik van revocation of expiration.

Risico	Bij het versleutelen van gegevens en het ondertekenen van berichten wordt gebruik gemaakt van sleutelparen. Een sleutelpaar zelf kent geen geldigheidsduur, maar geldigheidsduur kan worden aangegeven met certificaten. Wanneer in protocollen geen gebruik wordt gemaakt van de mogelijkheid voor certificaten om te verlopen of ingetrokken te laten worden door de uitgever ervan, is er geen mogelijkheid om het gebruik van sleutels die niet langer vertrouwd mogen worden te blokkeren. Deze zijn de facto dan 'eeuwig' geldig.
Analyse	Het mitigeren van dit risico is een belangrijk onderdeel van het protocol van Vorderingenoverzicht Rijk (Blauwe Knop Connect). Op korte termijn is het implementeren van expiration het eenvoudigst. Het nadeel daarvan is dat burgers tijdens het gebruik van de app het certificaat continu moeten vernieuwen, maar dat nadeel is te overzien. Op langere termijn is een vorm van privacy vriendelijke certificate revocation lists implementeren een waardevolle doorontwikkeling. Wat we aanvullend willen doen is de standaarden die bij Vorderingenoverzicht Rijk worden toegepast formaliseren en documenteren in standaardspecificaties.
Maatregelen	- Implementeren expiration. - Aanvullende maatregel (in samenhang met A06 en A07) Samen met een cryptograaf de toegepaste standaarden bij Vorderingenoverzicht Rijk formaliseren en documenteren.
Status	afgehandeld, expiration is geïmplementeerd. Op een later moment wellicht doorontwikkelen naar privacy friendly certificate revocation lists.

L07 RSA-sleutelparen worden niet gecontroleerd op sleutelgrootte

Risico	Wanneer sleutelparen niet op grootte worden gecontroleerd tijdens het uitvoeren van het protocol, is het mogelijk dat deelnemers bewust of onbewust te kleine sleutels gebruiken en daarmee de garanties die ondertekening en versleuteling kunnen bieden niet langer gelden, zodat gegevens niet meer afdoende worden beschermd.
Analyse	Het is belangrijk dit punt te mitigeren.
Maatregelen	Implementeren dat altijd eerst wordt gecontroleerd of een sleutelpaar van de minimale grootte is, voordat een sleutel gebruikt wordt.
Status	Afgehandeld

A04 Onversleutelde data in de API start_legalisation

Risico	Wanneer de public key van de server.
Analyse	Deze endpoint wordt altijd via HTTPS aangeroepen en is daarom binnen transport wel altijd versleuteld. Desalniettemin willen we ook bij dit endpoint een extra versleuteling toevoegen met de public key van de wederpartij, zodat deze gegevens end to end versleuteld zijn.
Maatregelen	Het bericht dat verstuurd wordt bij de start_legalisation endpoint versleutelen met de public key van de wederpartij.
Status	Afgehandeld

A05 Nonce is niet eenmalig geldig

Risico	Nonces (Numbers only used ONCE) worden in cryptografische protocollen gebruikt op plekken waar garanties nodig zijn dat het betreffende stukje informatie inderdaad maar één keer wordt gebruikt. Als het mogelijk is een en dezelfde nonce meerdere keren te gebruiken, dan wijst dit op een probleem in ofwel de naamgeving (de betreffende informatie is geen nonce) of in de implementatie.
Analyse	Dit betreft inderdaad een nonce die niet herbruikbaar mag zijn. Omdat het verwijderen van de nonce niet in de eerste stap van de verwerking gebeurt, kan het zo zijn dat de nonce in zeer korte tijd meerdere malen gebruikt wordt. Dit passen we aan.
Maatregelen	Implementeren dat de nonce direct wordt verwijderd bij gebruik, zodat dubbel gebruik onmogelijk is.
Status	Afgehandeld

A06 Niet gedefinieerd hoe de Json wordt gesigneerd

Risico	Indien twee partijen Json data op verschillende wijze opmaken (indentatie, sorteervolgorde etc.), kan het gebeuren dat door deze verschillen cryptografische operaties mislukken, terwijl wanneer er een standaard is afgesproken voor het gebruik van JSON in cryptografie alle partijen verplicht worden om JSON op dezelfde manier op te maken.
Analyse	We moeten inderdaad duidelijk specificeren welke standaard we gebruiken voor het gebruik van JSON in cryptografische operaties, zodat alle partijen dit op dezelfde manier uitvoeren.
Maatregelen	- Samen met een cryptograaf de toegepaste standaarden bij Vorderingenoverzicht Rijk formaliseren en documenteren (in samenhang met M06 en A07). - Zorgdragen dat in alle implementaties de standaarden worden nageleefd (in dit geval JSON Web Tokens (JWT).
Status	Afgehandeld

A07 Afhankelijkheid op (kopie van) fast-rsa

Risico	Het gebruik van externe cryptografie-libraries brengt een afhankelijkheid met zich mee op die libraries. Afhankelijkheid van een weinig gebruikte/ondersteunde cryptografielibrary is daarbij een risico omdat (veiligheids)updates wellicht niet.
Analyse	We onderschrijven deze risico's volkomen, en we gebruiken deze library vooral omdat hij het mogelijk maakt om relatief snel een werkende totaalslice van het systeem op te zetten binnen de agile werkwijze. We hebben de cryptografie implementatie die in fast-rsa gebruikt wordt onderzocht en zijn ons ervan bewust dat we die ook rechtstreeks zelf kunnen gebruiken in plaats van via de fast-rsa package. Iets dat we graag willen doorvoeren maar tot nu toe (we denken terecht) lagere prioriteit had op de backlog dan andere functionaliteiten, zeker omdat er aan de cryptografie nog het een en ander kon en kan veranderen.

Maatregelen	- Samen met een cryptograaf de toegepaste standaarden bij Vorderingenoverzicht Rijk formaliseren en documenteren (in samenhang met M06 en A06). - De cryptografie-implementatie vervangen door een directe native implementatie en fast-rsa uitfaseren.
Status	Onderhanden

Statusoverzicht bevindingen

Naam	Categorie	Status
L01 Ongeldig certificaat	Laag	Geen actie nodig
A01 Onnodige endpoints	Aandachtspunt	Geen actie nodig
L02 Beheerinterfaces kunnen achterhaald worden	Laag	Geen actie nodig
A02 Redirectdomein is niet geregistreerd	Aandachtspunt	Opgelost
M01 App heeft geen jailbreak-detectie	Middel	Mogelijk later
L03 Geen certificate pinning	Laag	Backlog
L04 Geen beveiliging tegen schermopnames	Laag	Mogelijk later
A03 Geen vergrendeling na time-out	Aandachtspunt	Backlog
M02 Geen toegangscontrole/biometrie	Middel	Backlog
L05 Private key wordt onversleuteld opgeslagen	Laag	Onderhanden
M03 Database-file (inclusief private key) is onversleuteld	Middel	Opgelost
L06 Database bevat onversleutelde data	Laag	Opgelost
M04 Database wordt niet verwijderd bij leegmaken app	Middel	Opgelost
M05 Database wordt meegenomen in back-ups	Middel	Mogelijk later
H01 Cumulatieve risico's van L05, M03, L06 en M05 samen	Hoog	Onderhanden
M06 Protocol bevat geen revocation of expiration	Middel	Opgelost
L07 Minimale sleutelgrootte wordt niet afgedwongen	Laag	Opgelost
A04 API call start_legalization is onversleuteld	Aandachtspunt	Opgelost
A05 Nonce is herbruikbaar	Aandachtspunt	Opgelost
A06 Geen standaard voor certificaatondertekening	Aandachtspunt	Opgelost
A07 Afhankelijkheid op externe cryptografie-implementatie	Aandachtspunt	Onderhanden

Bijlage | Geanonimiseerd rapport pentest Vorderingenoverzicht Rijk

Zie bijlage