**Bijlage 1 nota naar aanleiding van het verslag Wetsvoorstel Tijdelijke bepalingen in verband met de inzet van een notificatieapplicatie bij de bestrijding van de epidemie van covid-19 en waarborgen ter voorkoming van misbruik daarvan (Tijdelijke wet notificatieapplicatie covid-19)**

| ID | Organisatie | Titel | Omschrijving | CVSS-score | Status | Uitleg |
|---|---|---|---|---|---|---|
| RN1 | Secura | Decoy messages not disabled when Exposure notification is disabled. | The decoy upload scheduler does not seem to take the disabled status of the application in to account. While this is not a security vulnerability, it might be not intuitive for users of the application. | 3.7 | wordt verholpen | |
| RN2 | Secura | Outdated library used in iOS application: OpenSSL | CoronaMelder, Android and iOS application | 0.0 | Opgelost | |
| RN3 | Secura | The subject name in the certificate used for TEK signing is not checked. | When validating the second signature (using the certificate based CMS/PKCS# format) on a TEK list received by the server, the root and issuing CA certificates within the chain are checked. The subject name in the leaf certificate is not validated. | 1.9 | wordt verholpen | Deze wordt verholpen, zodra de HSM's operationeel zijn |
| NLC-019 | ROS | Identity Hub | The solution uses The Identity Hub (https://theidentityhub.com) as its OAuth provider to allow users access to the healthcare API. | 0.0 | Gesloten | Was gemarkeerd 'hoog'. Het is geen bevinding, maar een beschreven risico. Volgens FMEA zou deze scoren: ernst: 4 (slechte pers, datalek van omvang) voorkomen: 1 (identity hub is geen |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | onbekende partij) detecteerbaarheid: 3. RPN: 12 (klein), kritieke score: 4 (klein).<br><br>Deze authenticatiemethode is aangeschaft door de GGD/GHOR en is een professioneel bedrijf dat deze dienstverlening levert. De onderzoekers hebben louter gekeken naar de verwijzen. Er is niet gekeken naar het afsprakenkader, er is niet gekeken naar de implementatie of ander beveiligingsonderzoek gedaan.<br><br>Er is contact geweest met de GHOR om deze bevinding onder de aandacht te brengen. De keuze van het uitbesteden van deze dienst wordt echter niet direct als beveiligingsrisico gezien gelet op afsprakenkader en de professionaliteit van de dienstverlener. Het in eigen beheer uitvoeren van authenticatie zou niet automatisch de kwaliteit verhogen ten opzicht van een bedrijf dat hierin is gespecialiseerd.<br><br>Wel is de aanbeveling aanleiding hier in het beheersstadium samen met de GHOR nog wel onderzoek te naar laten doen. |

| | | | | | | |
|---|---|---|---|---|---|---|
| NLC-013 | ROS | API-feedback | HealthAuthorityEmployeesCanCheckIfKeysWere Uploaded | | wordt verholpen in kader livegang | Deze functionaliteit was voor testen, maar wordt verwijderd voor definitieve versie. |
| NLC-002 | ROS | Developer Options To Switch Off Security Features | DevelopmentOnlySettings.cs contains options to switch off security features such as the back-end's user authentication and use of HTTPS. The default is to have these security features switched on, which is good. As long as the option to switch off significant parts of the security features is present, however, these features might conceivably be turned off accidentally. | | Opgelost | |
| NLC-004 | ROS | RollingPeriod Not Limited To One Day | The RollingPeriod of uploaded keys is not properly checked. Uploaded keys can continue into the following days. | | Opgelost | |
| NLC-005 | ROS | It Is Possible to Update Diagnosis Keys With Future Dates | MobileAppApi does not check if an uploaded TEK is associated with a future date. | | Opgelost | |
| NLC-007 | ROS | Decoy Traffic Is Not Efficient | The decoy traffic analysis is not in line with the design and does | | wordt verholpen | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | not seem to be able to successfully mimic real traffic. | | | |
| NLC-014 | ROS | Authorization Token Included in GET Parameter | The JWT for authentication against the health authority back-end is part of a GET parameter. | | Opgelost | |
| NLC-017 | ROS | Databases have Insufficient Privileges Separation | Even though the databases are accessed by different programs with different needs, there is limited privilege separation. | | Opgelost | |
| NLC-018 | ROS | Signing Components Imply Running as Local Administrator | Some components imply they need to run as local administrator. If they do, their compromise would occur in the context of the administrator role instead of in that of an isolated process. | | Opgelost | |
| NLC-020 | ROS | Health Worker Authentication Token Is Valid For Several Hours and Not Rate-Limited | The JWT used for authentication is valid for several hours. There is no rate limiting nor any way to revoke individual authentications. | | Opgelost | |
| NLC-022 | ROS | HSTS Header Not Set | A HTTP Strict-Transport-Security response header (HSTS) is recommended for all APIs that only use SSL, in order to prevent adversaries from using | | Ondervangen door maatregel | A discussion with the developers revealed that HTTPS is terminated at the load balancer. This could mean this finding is invalid; we cannot confirm this in a |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | SSL stripping attacks in a MitM scenario. | | | code-only review. We do not recommend terminating HTTPS here, to prevent<br>information being available in plain text on the infrastructure network. |
| NLC-028 | ROS | Timing Oracle in Signature Comparison | The signature validation used during diagnosis key upload contains a timing oracle. | | Gesloten | Ofschoon dit in de database waar is, zou het aanpassen leiden tot het introduceren van nieuwe kwetsbaarheden. Zoals de ontdekker terecht aangeeft, is dit niet bewezen en een theoretische mogelijkheid met lage kans van slagen. Het introduceren van nieuwe problemen weegt niet op tegen het issue dat wordt verholpen |
| NLC-029 | ROS | AuthorizationCode is weak | The authentication against the health authority back-end contains a weak single-use component. | | wordt verholpen | |
| NLC-001 | ROS | Deviation Between (API) Design and Implementation | The architecture and design deviates from the implementation. Inconsistent documentation can be a source of errors<br>and confusion. | | wordt verholpen | |
| NLC-003 | ROS | Database Credentials in Components That | Connection strings containing database credentials are included in the appsettings.json | | Opgelost | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Do Not Require Them | of components/servers that do not require them. | | | |
| NLC-008 | ROS | Database Stores Upload and Phone Call Times Etc. | The database stores time values relating to diagnosis keys. In combination with other information, this can aid de-anonymization efforts. | | Opgelost | |
| NLC-009 | ROS | Log Messages Store Sensitive Information | The log messages store information which, together with log timestamps, can aid de-anonymization efforts. | | Opgelost | |
| NLC-010 | ROS | API Exceptions Are Too Verbose | Developer exception page function is activated in production. | | Opgelost | Deze bevinding betreft 'Security through Obscurity' |
| NLC-012 | ROS | JWT Token Not Properly Validated | Any valid JWT token is accepted as valid regardless of its properties. As this token needs to match the one stored in the database, this does not currently result in an issue. It could however result in confusion or issues in future updates. | | Opgelost | |
| NLC-015 | ROS | Database Provision Default Setting Is To Generate | The default configuration is to add example keys to the database. | | Opgelost | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Example Content | | | | |
| NLC-016 | ROS | Decoy Keys Can Largely Be Distinguished From Real Diagnosis Keys | The decoy keys added to increase anonymity can mostly be distinguished from real diagnosis keys by their properties. | | Opgelost | |
| NLC-021 | ROS | IccBackend API Allows CORS Requests From Any Source | The Cross-Origin Resource Sharing (CORS) policy facilitates Cross-Site Request Forgery (CSRF) attacks | | Opgelost | |
| NLC-023 | ROS | JWT Token Needlessly Contains Employee Information | JWT Token Needlessly Contains Employee Information | | Opgelost | |
| NLC-025 | ROS | Old Diagnosis Keys Are Not Deleted | Uploaded diagnosis keys are not deleted, only marked as published. | | Opgelost | |
| NLC-026 | ROS | Diagnosis Key Publishing Time Can Reveal the Time of the Phone Call | There is no intentional delay between the time of uploading and the time of publishing for diagnosis keys. | | Gesloten | Deze bevinding is correct alleen betekent het maken van een aanpassing extra vertraging. Omdat niet bekend is of de zieke direct een upload doet, het ook niet bekend is in welke regio het gesprek heeft plaats gevonden en iemand toegang moet hebben tot het betreffende GGD-systeem is de waarschijnlijkheid uiterst klein. Wat vervolgens bekend zou |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | kunnen worden is dat er sleutels zijn geupload niet welke sleutels dat betreft. |
| NLC-027 | ROS | Database Can Retain Data after Deletion | The Microsoft SQL database used in the background can retain data for longer than strictly required. | | Gesloten | De onderzoeker stelt vast dat het mogelijk zou zijn dat data te lang in de database kan staan. De technische review van de broncode onthult niet procedurele maatregelen en andere technische maatregelen. In de praktijk wordt de database geschoond en vindt er ook verificatie plaats. |
| NFIR 01 | NFIR | HTTP Security Headers – Meerdere headers | Voor de hosts zijn geen of niet alle HTTP Security headers ingesteld. Door het instellen van deze headers kunnen webbrowsers diverse kwetsbaarheden voorkomen. De volgende headers zijn gecontroleerd:<br>• HTTP Strict Transport Security (HSTS): Header die het gebruik van HTTPS forceert.<br>• X-Frame-Options: Geeft een melding aan de browser of de site in een frame geladen mag worden of niet. Met deze header kunnen clickjacking aanvallen voorkomen worden, aangezien de site niet in een frame geladen kan worden. Als | 7.5 | Opgelost | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | een aanvaller de site wel in een frame zou kunnen laden, kan de aanvaller de gebruiker onbedoeld omleiden naar een malafide website.<br>• X-Content-Type-Options: Voorkomt dat een MIME-sniffing-aanval kan worden uitgevoerd, waarmee een aanvaller een bestand kan verbergen als een ander bestandstype. Hierdoor kan een malafide bestand bijvoorbeeld worden geüpload met een jpg-extensie. Doordat het bestand de kenmerken heeft van een legitiem, uitvoerbaar bestand, wordt de applicatie in sommige gevallen opgeslagen en uitgevoerd.<br>• Content-Security-Policy: Header die een site beschermt tegen Cross-site scripting (XSS) aanvallen. Door het definiëren van een lijst met toegestane content, kan je voorkomen dat de browser kwaadwillende code kan laden van een externe bron. Met de kwaadwillende code kunnen bijvoorbeeld cookies van gebruikers worden afgevangen | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | en gebruikt om mee in te loggen, of om malware te injecteren in de website.<br>• Referrer-Policy: Header die controleert welke informatie door een site opgehaald mag worden van een andere bron.<br>• Feature-Policy: Header waarmee controle is over welke functies en API's gebruikt kunnen worden in de browser.<br>Er is vastgesteld dat bij bovengenoemde hosts een of meerdere van deze zes security headers niet zijn ingesteld. | | | |
| NFIR 02 | NFIR | TLS v1.0 en v1.1 protocol ondersteuning (WSTG-CRYP-01) | De host ondersteunt de onveilige TLS-versies 1.0 of 1.1. Deze protocollen zijn sinds maart 2020 end-of-life en worden daarom niet meer ondersteund door de meest gebruikte browsers.<br>Het CDN-endpoint (https://productie.coronamelder-dist.nl/) wordt volgens de publieke documentatie1 door de CoronaMelder-applicatie voor iOS en Android gebruikt om publiek beschikbare informatie op te halen, waaronder bijvoorbeeld Diagnosis Keys | 6.7 | Ondervangen door maatregel | Bij het ontwerp werd al voorzien dat een content delivery network een dergelijk bevinding zou triggeren. Daarom worden DK's voorzien van een ondertekening met een PKI Overheids-cerrtificaat. De dreiging van integriteit en authenticiteit is daarmee ondervangen.<br>Voor vertrouwelijkheid speelt geen probleem, omdat de DK's naar hun aard Openbaar zijn. Juist het verdelen van deze sleutels is een kern-functionaliteit van de app. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | (DKs), die apart voorzien zijn van een digitale handtekening. | | | |
| NFIR 03 | NFIR | JWT Token blijft tot 3 uur geldig na uitloggen | De JWT token van een gebruiker blijft geldig voor een periode van 3 uur, vanaf het moment dat er uitgelogd is van de applicatie via de uitlogfunctionaliteit. Hierdoor kan er gedurende deze 3 uur opnieuw van deze JWT-token gebruik worden gemaakt om toegang te verkrijgen tot de applicatie | 6.6 | Opgelost | |
| NFIR 04 | NFIR | Denial of Service - Secure Client-Initiated Renegotiation | Secure Client-Initiated Renegotiation maakt het mogelijk om op een veilige manier te onderhandelen tussen de client en de host tijdens SSL-connecties. Een aanvaller kan honderden van deze onderhandelingen starten, en zo de host onbereikbaar maken door middel van een Denial of Service (DoS). | 6.1 | Opgelost | |
| NFIR 05 | NFIR | Kwetsbare ciphers waargenomen | De host stelt kwetsbare ciphers beschikbaar, welke mogelijk kwetsbaar zijn voor een kwetsbaarheid genaamd BEAST | 5.2 | Ondervangen door maatregel | Dit is al in de ontwerpfase als potentiële dreiging onderkend. Door aanvullende ondertekening te bieden, wordt dit probleem ondervangen. Het inzetten van HSM's biedt hier de |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | – deze kwetsbaarheid draagt het CVE-nummer CVE-2011-3389. | | | oplossing om dit probleem volledig te mitigeren en een hoger niveau van beveiliging te bieden dan een dienstverlener had geboden. |
| NFIR 06 | NFIR | Niet-versleutelde HTTP-verbinding | De webserver ondersteunt HTTP. Hierdoor wordt data over een niet-versleutelde verbinding naar de webserver gestuurd. | 4.8 | Opgelost | |
| NFIR 07 | NFIR | Testomgeving vindbaar via Google | De testomgeving van het meldportaal is beschikbaar via internet. Daarnaast is deze testomgeving geïndexeerd door Google. | 4.8 | Opgelost | |
| NFIR 08 | NFIR | Informatie in foutmeldingen en headers | De webserver geeft veel informatie vrij bij foutmeldingen, waardoor het aanvalsoppervlak voor een potentiële aanvaller wordt vergroot. | 4.4 | Opgelost | |
| NFIR 09 | NFIR | Sessie is niet gebonden aan IP-adres | De webapplicatie kijkt niet of voor een actieve sessie het publieke IP-adres gewijzigd is. De sessie blijft actief en er wordt niet gevraagd om extra validatie. | 4.4 | Open | "Dit probleem is onderkend, maar complex om op te lossen. Omdat het daadwerkelijk uitvoeren van een succesvolle aanvallen complexer is en daarna vervolgens maar beperkte impact zal zijn in de executie. Zelfs als het lukt om in te loggen is de impact beperkt. Zelfs na het doorzetten van sleutels is het veel werk om |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | daadwerkelijk een melding te activeren.<br>Het probleem wordt echter wel Opgelost en is daarom aan de back log toegevoegd." |
| NFIR 10 | NFIR | Angular Development modus ingeschakeld | De webapplicatie die gehost wordt op coronamelder-portal.nl is geconfigureerd om in de ‘development modus’ te worden uitgevoerd. | 3.8 | Opgelost | |
| NFIR 11 | NFIR | Access-Control-Allow-Origin configuratie | Cross Origin Resource Sharing (CORS) is een HTML5-technologie die moderne webbrowsers de mogelijkheid geeft om beperkingen te versoepelen die standaard zijn geïmplementeerd door het Same Origin-beleid.<br>De 'Access-Control-Allow-Origin'-header is onveilig geconfigureerd wanneer deze is ingesteld op ‘*’ of null, omdat de header er dan voor zorgt dat elk domein het toestaat om cross-domein verzoeken uit te voeren en de reacties uit te lezen. | 3.8 | Opgelost | |
| NFIR 12 | NFIR | Invoervalidatie onvolledig | De API controleert de invoer niet op tekens die een speciale | 0.0 | Opgelost | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | betekenis hebben in HTML en JavaScript. | | | |
| NFIR 13 | NFIR | Verouderde SSL-bibliotheek aanwezig | De COVID-19 Notificatie applicatie voor Apple iOS (buildnummer 1.0.0 – 644f133) maakt voor het verwerken van data vanaf internet gebruik van een verouderde externe software- bibliotheek (OpenSSL versie 1.1.1d). Deze software-bibliotheek is mogelijk kwetsbaar voor een Denial-of-Service (DoS) aanval. Deze kwetsbaarheid draagt het CVE-nummer: CVE-2020-1967. | 6.9 | Opgelost | |
| NFIR 14 | NFIR | Cache aanwezig in app-container | De COVID-19 Notificatie applicatie voor Apple iOS (buildnummer 1.0.0 – 644f133) maakt voor het verwerken van data-sleutels gebruik van verschillende mappen binnen de applicatie- container. Na het verwerken van deze sleutels, blijven de cache-bestanden aanwezig binnen de applicatie-container. | 5.6 | Open | Dit probleem is aangemeld bij Apple. |
| NFIR 15 | NFIR | Jailbreak detectie niet aanwezig | De COVID-19 Notificatie applicatie voor Apple iOS (buildnummer 1.0.0 – 644f133) | 3.7 | Gesloten | Dit is een bewuste keuze. Door telefoons met jailbreak af te sluiten, sluiten we een doelgroep uit. Ook biedt |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | detecteert niet of het apparaat waarop de applicatie geïnstalleerd is, voorzien is van een zogenoemde “jailbreak”. | | | het hebben van een jailbreak mensen de mogelijkheid te controleren dat de app niks anders is dan de Open-sourcebroncode laat zien. |
| NFIR 16 | NFIR | Reverse Engineering Tools detectie | De COVID-19 Notificatie applicatie voor Apple iOS (buildnummer 1.0.0 – 644f133) detecteert niet of het apparaat waarop de applicatie geïnstalleerd is, reverse engineering tools zoals Frida bevat. | 2.7 | Gesloten | Er is geen geheim op de werking van de app. Reverse engineering kan leiden tot de bevestiting dat de broncode die publiekelijk beschikbaar is overreenkomt met de geinstalleerde software. Het is daarom zelfs wenselijk dat reverse engineering niet onmogelijk wordt gemaakt. Er is bewust gekozen om niet te beveiligen. op basis van security through obscurity. |
| NFIR 17 | NFIR | Emulator detectie niet aanwezig | De COVID-19 Notificatie applicatie voor Apple iOS (GitHub versie - buildnummer 1.0.2) detecteert niet of het apparaat waarop de applicatie geïnstalleerd is, een zogenoemde emulator betreft. | 0.0 | Gesloten | Inherent aan Open source code is dat de functionaliteit ook op andere devices werken met aangepaste functionaliteit. Zo draait het ook op niet-telefoonplatformen. Daarnaast is security through obscurity bewust iets wat niet wordt gedaan |
| NFIR 18 | NFIR | Informatie in schermafdruk | iOS apparaten bevatten de mogelijkheid om een schermafdruk te maken terwijl de applicatie op de achtergrond actief is. Hiermee kan mogelijk gevoelige data worden opgeslagen in een schermafdruk. | 0.0 | Gesloten | Omdat sommige gebruikers moeite hebben om te communiceren, kan een schermafdruk ze helpen. Op verzoek GGD'en. De risico's worden beperkt door het inzetten van wetgeving om misbruik hiervan te voorkomen en te bestraffen. |

| | | | | | | |
|---|---|---|---|---|---|---|
| NFIR 19 | NFIR | Cache aanwezig in app-container | De CoronaMelder applicatie maakt voor het verwerken van de gepubliceerde TEK-sleutels gebruik van verschillende mappen binnen de applicatiecontainer. Na het verwerken van deze sleutels, blijven de cache-bestanden aanwezig binnen de applicatie-container. | 5.6 | Opgelost | |
| NFIR 20 | NFIR | Root detectie niet aanwezig | De CoronaMelder applicatie voor Google Android detecteert niet of het apparaat waarop de applicatie geïnstalleerd is, voorzien is van een zogenoemde “root-toegang”. | 3.7 | Gesloten | Dit is een bewuste keuze. Door telefoons met jailbreak af te sluiten, sluiten we een doelgroep uit. Ook biedt het hebben van een jailbreak mensen de mogelijkheid te controleren dat de app niks anders is dan de Open-sourcebroncode laat zien. |
| NFIR 21 | NFIR | Reverse Engineering Tools detectie | De CoronaMelder applicatie voor Google Android detecteert niet of het apparaat waarop de applicatie geïnstalleerd is, reverse engineering tools zoals Frida en Drozer bevat. | 3.7 | Gesloten | Er is geen geheim op de werking van de app. Reverse engineering kan leiden tot de bevestiting dat de broncode die publiekelijk beschikbaar is overreenkomt met de geinstalleerde software. Het is daarom zelfs wenselijk dat reverse engineering niet onmogelijk wordt gemaakt. Er is bewust gekozen om niet te beveiligen. op basis van security through obscurity. |
| NFIR 22 | NFIR | Emulator detectie niet aanwezig | De CoronaMelder applicatie voor Google Android detecteert niet | 0.0 | Gesloten | Inherent aan Open source code is dat de functionaliteit ook op andere devices |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | of het apparaat waarop de applicatie geïnstalleerd is, een zogenoemde emulator betreft. | | | werken met aangepaste functionaliteit. Zo draait het ook op niet-telefoonplatformen. Daarnaast is security through obscurity bewust iets wat niet wordt gedaan |
| NFIR 23 | NFIR | Voorspelbare willekeurigheid | De CoronaMelder applicatie voor Google Android maakt twee keer gebruik van de voorspelbare Random()-functie. Deze functie is minder willekeurig (en daarmee minder veilig)dan de SecureRandom()-functie. | 0.0 | Gesloten | De waarde wordt gebruikt om verplichte opvulling (padding) aan te leveren. Het dient geen doel om te anonimiseren of codes weer te geven. Veilige willekeurige getallen zijn geen doel. Een aanpassing levert daarom niets op. |
| NFIR 24 | NFIR | WAKE_LOCK-permissie | De CoronaMelder applicatie voor Google Android maakt gebruik van de WAKE_LOCK- permissie. Deze permissie zorgt ervoor dat de processor actief blijft en het scherm niet gesluimerd kan worden. In de applicatie is geen functionaliteit aangetroffen waarvoor deze permissie noodzakelijk is. | 0.0 | Gesloten | Deze permissie is noodzakelijk voor het actief blijven van CoronaMelder. Dit heeft internationaal de aandacht. |
| NFIR 25 | NFIR | Apparaat beveiligingsbeleid opties | De applicatie controleert niet of één van de volgende beveiligingsinstellingen aanwezig zijn:<br>- Pincode of wachtwoord om het apparaat te ontgrendelen<br>- USB Debugging | 0.0 | Gesloten | Dit is een bewuste keuze, omdat anders gebruikers worden uitGesloten en veel complexiteit voor de gebruiker wordt toegevoegd. Het niet afsluiten van de telefoon is een taak van de gebruiker. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | - Apparaat Encryptie<br>Het risico dat een ongeautoriseerde gebruiker toegang kan verkrijgen tot het apparaat is hiermee verhoogd | | | |