To: (10)(2e))[(10)(2e) @minvws.nl]
From: (10)(2e)
Sent: Tue 9/29/2020 8:19:48 AM
Subject: Re: Opvallende punten
Received: Tue 9/29/2020 8:20:58 AM
20200928 Duidingsrapportage Coronamelder.pdf
Bijlage I - Codereview Radically Open Security.pdf
Bijlage K - Rapportage Penetratietest.pdf

Hoi,

Hier alles.

Groet,

(10)(2e)

Op 29-09-2020 om 10:17 schreef (10)(2e)):

> Dank! Mag ik ook de onderliggende rapporten voor de zekerheid?
>
> **Van:** (10)(2e) <(10)(2e)@ (10)(2e) com>
> **Verzonden:** dinsdag 29 september 2020 10:13
> **Aan:** (10)(2e)) < (10)(2e) @minvws.nl>
> **Onderwerp:** Opvallende punten
>
> (10)(2e)
>
> Eventjes mijn persoonlijke beleidsopvatting. Ik zie geen problemen in de bevindingen. Niet voor niets is mijn advies positief. Dat ligt op andere dossiers wel anders. Kortom niets is heel gevoelig. (10)(2a)
> (10)(2a)

het enige punt is NLC-019:

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). Deze authenticatiemethode is aangschaft 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. 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. Wel is de aanbeveling aanleiding hier in het beheersstadium samen met de GHOR nog wel onderzoek te naar laten doen.

Daar ga ik ook op in;

Een bevinding betreft bespreking en dat is de bevinding van Radically Open Security (NLC-019). Voor het aanmelden van medewerkers van de GGD maakt de GHOR gebruik van The Identity Hub als leveranciers om medewerkers te laten aanmelden. Voor de onderzoeker is uit de broncode van de software niet af te leiden welk afspraken kader met de leverancier gemaakt zijn. Omdat ze dat niet weten en toch willen waarschuwen ze hiervoor. Omdat het hacken van een toegangscontrole ernstige gevolgen zou kunnen hebben is dit gemarkeerd als 'hoog'. Het betreft geen technische tekortkoming. De onderzoekers schrijven zelf ook:

> *Using third party authentication components can be a valid choice, but from a code review perspective it adds another attack path, so we included it as a finding.*

Wat hier benoemd is, betreft een risico. Uit de FMEA-inschatting blijkt dat we vooralsnog dit als laag inschatten. Het beschreven alternatief (de GHOR zelf authenticatie laten regelen) leidt niet automatisch tot een lager risico. Dat neemt niet weg dat VWS dit onder de aandacht van de GHOR heeft gebracht. In het vervolgtraject zal hier nader naar worden gekeken.

Wat ROS niet als groot zag, maar ik wel:

NLC-013	ROS	API-feedback	HealthAuthorityEmployeesCanCheckIfKeysWere Uploaded		wordt verholpen	Deze functionaliteit was voor testen, maar wordt verwijderd voor definitieve versie.

Deze is het verhaal van was voor testen, maar moet er dus echt uit. Good find.

Een andere find is niet waarschijnlijk, maar kan wel gevoelig liggen:

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.

Tot slot deze, die is slim door ons ondervangen door een andere maatregel.

NFIR02	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. 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 (DKs), die apart voorzien zijn van een digitale handtekening.	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 onder-teke-ning met een PKI Over-heids-cerrtificaat. De dreiging van integriteit en authenticiteit is daarmee ondervangen. Voor ver-trouwelijk-heid 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.

--

(10)(2e)

(10)(2e)

(10)(2e)

--

(10)(2e)

(10)(2e)

(10)(2e)