Van: [redacted]@tweedegolf.com>
Verzonden: donderdag 20 augustus 2020 15:48
Aan: [redacted]@nijmegen.nl>
CC: [redacted]@tweedegolf.com>; [redacted]
<[redacted]@tweedegolf.com [redacted]@oblcc.com
Onderwerp: Re: feedback dongit

Hoi [redacted], [redacted],

Ik zie dat we het mogelijk niet goed gedocumenteerd hebben maar we hebben een hier een optie voor: Naast de listen-address is er ook de internal-address optie. Als je die op een andere poort zet komt de /call alleen daar op beschikbaar. Op die manier kan je met behulp van een firewall ofzo die internal port alleen benaderbaar maken vanuit de lambda.

[redacted]

On Thu, Aug 20, 2020 at 3:12 PM [redacted] <[redacted]@nijmegen.nl> wrote:

Ha,

Ik ben er even ingedoken, maar hier moeten we maandag nog wel even naar kijken.
De backend endpoints /call /disclose en /session zijn vanaf het publieke internet benaderbaar (de hele container is in feite vanaf het internet toegankelijk via http(s)).
Er is in de setup geen sprake van een nginx oid, wel een loadbalancer, zie plaatje.

@[redacted]: als ik het niet goed zie hoor ik het graag.

Als ik [redacted] goed begrijp, en dat klinkt ook logisch, moeten we zorgen dat /disclose en /session/update vanaf het publieke internet toegankelijk zijn (vanuit de agent pagina en voor de belknop zelf)

/call zou alleen toegankelijk moeten zijn vanuit de Lambda functie.

Klopt dat?

Zijn we er als we zorgen dat /call alleen vanuit de Lambda te benaderen is?

@[redacted]: is dat realiseerbaar in de huidige setup, dat alleen /disclose en /session vanaf het publieke internet te bereiken zijn en /call alleen vanuit de lambda?

Groeten,

[redacted]

Van: [redacted] <[redacted]@tweedegolf.com>
Verzonden: vrijdag 14 augustus 2020 09:12
Aan: [redacted] <[redacted]@nijmegen.nl>; [redacted] <[redacted]@tweedegolf.com>; [redacted] <[redacted]@tweedegolf.com>
Onderwerp: Re: feedback dongit

Hoi [redacted],

Ik denk dat [redacted] en [redacted] beter in staat zijn dan ik om hier een antwoord op te geven. Wel is het zo dat er inderdaad onderscheid gemaakt moet worden tussen externe (publiek toegankelijke) en interne (slechts vanaf de eigen infrastructuur) endpoints. Ik heb de beoordeling van [redacted] even vluchtig doorgelezen, en heb het idee dat hij het verschil daartussen niet helemaal duidelijk heeft. De beveiliging van de interne endpoints is gebaseerd op het niet-publiek toegankelijk zijn ervan. Deze interne endpoints staan vanuit het perspectief van de backend gewoon open, maar worden afgesloten door andere onderdelen op het netwerk (zoals nginx).

Laten we het inderdaad nog even bespreken. Ik heb dit punt vast op de agenda gezet.

Groetjes,

[redacted]

On Fri, Aug 14, 2020 at 8:06 [redacted] <[redacted]@nijmegen.nl> wrote:

Dag heren,

Onderstaand de technische bevindingen van Dongit.
Zoals je ziet heb ik al wat discussie gehad met ze ;-).

Denk er maar even over na hoe we hier verstandig mee om kunnen gaan, en wat we echt op moeten lossen, en wat er uitgelegd kan worden.

Maandag de 24e kunnen we het er dan over hebben (wat eerder mag ook als dat handiger is, maar dat hangt ook van jullie beschikbaarheid af).

Groeten,

[redacted]

Van: [redacted] <[redacted]@dongit.nl>
Verzonden: donderdag 13 augustus 2020 15:43
Aan: [redacted] <[redacted]@nijmegen.nl>
CC: [redacted] <[redacted]@dongit.nl>; [redacted] | DongIT <[redacted]@dongit.nl>
Onderwerp: Re: voortgang testen en eventuele technische issues

Dag [redacted],

Bedankt voor je uitleg.

1) Streng gezien hoeft voor de bestaande functionaliteiten maar /session (om een sessie aan te maken) publiek beschikbaar te zijn. Het publiek beschikbaar maken van de rest van de eindpunten brengt risico's in dat zou ik niet zonder reden doen. Vanuit de code had ik de indruk, dat het wel de bedoeling was om hier een onderscheid te maken tussen intern en extern. Via /call kan bvb gechecked worden of een dtmf code bestaat en het bijhorende secret opgehaald worden. Met 1E10 requests kan elke mogelijke code gechecked worden. Dit is iig geen gek hoog getal. Niet als er misschien 1000 actieve sessies bestaan (verwachte aantal requests daalt om een valide code te vinden). Zeker niet in een potentieel "infinitely scalable" cloud omgeving in de komenden jaaren. Hier zouden wij ten minsten aanbevelen om een rate-limiting in te bouwen.

2) Dat is een valide reden om het niet via connect te laten gaan. Hier moet wel over nagedacht worden, hoe de requests beter kunnen beveiligd woorden. Iig zouden wij aanbevelen om de secrets niet als GET parameter te versturen, want urls woorden misschien in Browser history opgeslagen. Maar ik begrijp dat jullie hiervoor geen verder uitleg nodig hebben.

3) Wij bedoelen de belknop. Die kan gekopieerd worden om burgers op een phishingsite met de backend en IRMA te laten authenticeren. Vervolgens heeft de opzetter van de phishingsite toegang tot DTMF code, Secret en IRMA attributen en kan vervolgens inbellen als het slagtoffer. Wij zijn nog aan het nadenken over mogelijke oplossingen hiervoor.

4) Is gerelateerd aan 3). Als de website waar de inlbelbutton neergezet wordt, bvb een cross-site scripting kwetsbaarheid bevat, komt in principe het hele DOM onder kontrole van de attacker en je hebt hetzelfde probleem als bij 3).

5) Wel 'geen manier'. Wij zouden dus aanbevelen, om geen eindpunt beschikbaar te stellen war gechecked kan worden of een DTMF code geldig is. Want die kan altijd gebruik worden om in te bellen, ook als de bijhorende attributen voor een attacker niet bekend zijn.

Als er nog vragen zijn hoor ik het graag!

Ik heb nog een vraag van mij kant. Je had de terraform code voor ons klaar gezet (https:// [redacted]), maar toen zei je dat er nog wat modules ontbreken, en je dit zou kunnen oplossen, als je er weer bent. Zou je de gehele terraform code voor ons beschikbaar kunnen maken?

Alvast bedankt!

Groeten,

[redacted]

DongIT
[redacted])
Developer & Pentester

T: +31 (0)71 [redacted]
E: [redacted]@dongit.nl
L: [redacted]
W: www.dongit.nl | www.websecurityscan.eu

On Thu, Aug 13, 2020 at 2:13 PM [redacted] <[redacted]@nijmegen.nl> wrote:

Dag [redacted],

Bedankt voor je mail.

Een paar opmerkingen / vragen:

1. Ze zijn bewust niet dichtgezet. Het idee is dat het secret niet binnen 1 uur 'gekraakt' kan worden. Na max 1 uur zijn de onthulde gegevens verwijderd uit de back-end database, en met de volgende release al eerder, zodra de agent op 'clear contact' heeft gedrukt.
Zien jullie problemen met deze constructie? Is jullie inschatting dat het wel haalbaar is om binnen 1 uur 'beet' te hebben met een 'zelfgemaakt' secret?
Een feature dus ;-). Maar jullie constatering is nog steeds een terechte, en we zullen op z'n minst goed moeten uitleggen waarom ze niet afgeschermd zijn.

2. Dat is ook een design beslissing; Op deze manier worden de persoonsgegevens niet 'rondgepompt' en komen dus ook niet in de Connect omgeving (of in een later stadium in een andere telefonie centrale) terecht, en daardoor misschien ook veel sneller in bijvoorbeeld logging tevoorschijn.

We werken nu vanuit pragmatisch perspectief met Connect, maar het moet uiteindelijk implementeerbaar zijn in een gemeentelijk telefonie systeem, wat daar gebeurt willen we dus zo eenvoudig mogelijk houden om de kans te vergroten dat het ergens anders ook werkend te krijgen is. In Connect kunnen we de gegevens misschien nog wel goed beschermen, maar het principe moet ook werken met andere telefonie systemen waar dit misschien wel een probleem is.

Ik ben benieuwd wat jullie hiervan vinden.

3. Welke front-end bedoel je hier? De knop/javascript waar een inwoner op klikt, of de webpagina waar de kcc medewerker het telefonie deel in afhandelt?
En wat voor soort/type maatregelen moeten we hier dan aan denken?

4. Ik snap een beetje wat je hier zegt, maar het zou helpen als je hier een paar zinnen meer aan kunt wijden zodat het iets minder cryptisch is ;-)

5. Je bedoelt ‘een manier’ neem ik aan, en niet ‘geen manier’.
Als iemand een ongeldige (zelfbedachte) dtfm code meestuurt dan kan er geen sessie gevonden worden in de backend en loopt het proces spaak.
Welk gevaar zien jullie hier, waartegen zou het valideren van een dtfm moeten helpen?

Groeten,

[redacted]

Van: [redacted] <[redacted]@dongit.nl>
Verzonden: donderdag 13 augustus 2020 12:25
Aan: [redacted] <[redacted]@nijmegen.nl>
CC: [redacted] <[redacted]@dongit.nl>; [redacted] | DongIT <[redacted]@dongit.nl>
Onderwerp: Re: voortgang testen en eventuele technische issues

Beste [redacted],

Wij zijn bijna klaar met het testen en hebben een aantal verbeterpunten gevonden. Hiervan zijn de belangrijk in het kort de volgende:

1) Wij hebben access control issues gevonden met betrekking tot de backend server. Al de eindpunten op de backend server blijken publiek toegankelijk te zijn, onder anderen ook /call (om een DTMF code tegen een irma secret uit te wisselen) die expliciet niet toegankelijk zou moeten zijn.

2) Voor ons is het niet helemaal duidelijk waarom bij een inkomend gesprek in de connect omgeving de DTMF code door de lambda functie uitgewisseld wordt voor een IRMA secret. Vervolgens worden de IRMA attributen pas in het connect frontend (dev.irma-bellen.nl) opgehaald. Dit heeft namelijk als gevolgd dat nog een eindpunt publiek toegankelijk dient te zijn welke de meest gevoelige informatie teruggeeft. Ons voorstel zou zijn om de IRMA attributen meteen terug te geven waar nu door de Lambda functie alleen het irma secret wordt teruggegeven. Dat heeft twee voordelen. De attributen worden niet meer door een publiek beschikbaar eindpunt teruggegeven en de attributen kunnen alleen maar ingezien worden door iemand met een ook geldige aws connect sessie i.p.v. alleen het irma secret.

3) Er zijn geen maatregelen genomen om te voorkomen, dat de JavaScript front-end op een andere server gebruikt kan worden, om bijvoorbeeld een phishing server op te zetten die met de bestaande backend systemen gekoppeld wordt.

4) In het bestaande voorstel is de "confidentiality" van de DTMF code en een bijhorend IRMA secret, afhankelijk van de beveiliging situatie op de website waar de button wordt geplaatst (cross-site scripting kwetsbaarheden).

5) De DTMF code is de enige parameter die een inkomend gesprek aan IRMA attributen linked. Er moet dus geen manier bestaan om voor het inbellen te checken of een DTMF code geldig is.

Ik probeer tot eind van de dag nog meer informatie door te geven m.b.t. bevinding 2. Dit is volgens mij de meest ingrijpende wijziging als jullie dit zouden oppakken.

Groeten,
[redacted]

DongIT
[redacted]
Developer & Pentester

T: +31 (0)71 [redacted]
E: [redacted]@dongit.nl
L: [redacted]
W: www.dongit.nl | www.websecurityscan.eu

On Thu, Aug 13, 2020 at 10:04 AM [redacted] | DongIT <[redacted]@dongit.nl> wrote:

Kan je [redacted] voorzien van een update?

---------- Forwarded message ---------
From: [redacted] <[redacted]@nijmegen.nl>

Date: Thu, Aug 13, 2020, 09:42
Subject: voortgang testen en eventuele technische issues
To: [redacted]@dongit.nl <[redacted]@dongit.nl>
Cc: [redacted] <[redacted]@nijmegen.nl>

Dag [redacted],

Is het gelukt / lukt het met testen?

Je hebt aangegeven dat als jullie technische dingen tegenkomen die opgelost moeten worden jullie dat door konden geven voor we de rapportage zelf ontvangen, zodat de externe ontwikkelaars dat mee kunnen nemen in de tijd die we nu ingepland hebben voor ze.

Zijn jullie iets tegengekomen dat opgelost moet worden? Als ik het begin volgende week weet dan hebben we nog tijd om het mee te nemen.

Groeten,

[redacted]

--

[redacted]

M: +316 [redacted]

T: +3124 [redacted]