Pulsesecure Breach

Koen Colpaert

August 13, 2020

1 *<2020-08-13 Thu>*

1.1 Aanwezigen

Naam	Organisatie	Rol
Koen Colpaert	FenB	CISO
Peter Van den Neucker	FenB	CIO
Ward Bemelmans	FenB	Staf
Tom Janssens	FenB	Systemen
Aimad Soultani	FenB	Netwerk
Younes Fourir	Proximus	GCA/SGI

1.2 Reeds Ondernomen acties

- Younes geeft de laatste stand van zaken. Op basis van zijn bevindingen hebben we de bewijzen dat er ongeoorloofde toegang is geweest en dat er gevoelige data werd gestolen. Er is evenwel geen code uitgevoerd. Diegenen die de vulnerability hebben misbruikt hebben geen verdere acties genomen, nadien zijn er wel vanuit verschillende landen pogingen geweest om aan te melden maar aangezien we voor het overige een goede configuratie hadden is dat niet gelukt.

- Op basis van deze informatie werd besloten het onderzoek hier te stoppen. Younes levert een eindrapport op en we bekijken ism Proximus wat we met de resterende dagen kunnen doen. Verschillende pistes zijn mogelijk: training on the job, red team of opsparen voor latere cases.

1.3 Te ondernemen acties

- Younes neemt contact op intern om te zien welke opties we hebben voor de resterende dagen

- Koen zal deze vraag officieel stellen via mail
- Koen annuleert de stavaza meeting van morgen
- De LDAP bind en het opbrengen van de cluster dienen te worden opgenomen in de planning van het netwerkteam
- De staf zal zich in de loop van volgende week buigen over de nodige acties voor het instellen van processen en organisatie

1.4 Communicatie

- er werd geen verdere communicatie gepland. We wachten het eindrapport Proximus af, in tussendtijd kan dit document gebruikt worden voor de communicatie naar het management.

2 *<2020-08-12 Wed>*

2.1 Aanwezigen

Naam	Organisatie	Rol
Koen Colpaert	FenB	CISO
Peter Van den Neucker	FenB	CIO
Tom Janssens	FenB	Systemen
Ward Bemelmans	FenB	Staf
Aimad Soultani	FenB	Netwerk
Younes Fourir	Proximus	GCA/SGI
Dirk Van Der Sanden	DXC	
Renaud Dubois	HBplus	

2.2 Reeds Ondernomen acties

- Younes geeft een overzicht van zijn bevindingen in Splunk op de VPN logs. Er zijn verschillende logins geweest vanuit diverse landen maar na contact met de betrokken gebruiker/dienst bleek dat telkens om legitieme aanmeldingen te gaan. Uiteindelijk werd de lijst terug gebracht tot 6 verschillende pogingen uit Japan en Rusland maar geen enkele raakte verder dankzij onze MFA.
- De paswoorden voor de Radius en AD werden aangepast zodat ook daar mogelijk misbruik uitgesloten is.

- De reset van de gebruikerspins is een voortdurend proces
- Alle korte termijn acties (reset pins, SSH, lokale accounts,. . .) werden daarmee afgehandeld
- Younes stelt de vraag of -in het licht van de bevindingen van de VPN logs- het nog nodig is hierop verder te gaan. We kunnen ondertussen redelijk uitsluiten dat er langs daar verdere niet-geauthoriseerde toegang was? Er wordt donderdag 13/8 een aparte meeting gehouden om de strategie op korte termijn te bepalen.

2.3 Te ondernemen acties

- De HD werd gecloned en wordt op 13/8 terug geplaatst
- FenB kan vanaf dan beginnen met het terug opbrengen van de cluster en de opkuis van de gebruikersaccounts
- Verder forensisch onderzoek zal zich toespitsen op de logs van de firewall
- LDAP simple bind wordt aangepast zodat er niets meer in clear-text wordt overgestuurd

2.4 Communicatie

- Koen stelt een mail op voor Koen A en David VH met een stand van zaken en een overzicht van de uitgevoerde en nog uit te voeren acties.

3 *<2020-08-10 Mon>*

3.1 Aanwezigen

Naam	Organisatie	Rol
Koen Colpaert	FenB	CISO
Ward Bemelmans	FenB	Staf
Peter Van den Neucker	FenB	CIO
Tom Janssens	FenB	Systemen
Renoud Dubois	HBplus	
Dirk Van Der Sanden	DXC	
Bart Cober	Proximus	1IT/ESE
Aimad Soultanin	FenB	Netwerk
Younes Fourir	Proximus	GCA/SGI

3.2 Reeds ondernomen acties

- AD en LDAP sync accounts werden aangepakt. LDAP werd gereset en AD stond al disabled.
- Er wordt gevraagd naar clear text protocols; volgens Aimad is alles SSL encrypted. Vraag is of dat ook zo is voorbij de VPN?
- Status pins: alle users disabled, communicatie uitgestuurd. Software token krijgt nieuwe PIN, hardware token wordt terug geactiveerd. Hardware token is wat omslachtige procedure, uitschrijven voor de toekomst
- Uit een eerste analyse van de logs komen alvast enkele onverklaarbare cases naar voor. Lijst van deze gebruikers wordt overgemaakt aan FenB voor checken van de accounts in AD. Ook al zijn er aanmeldingen van verschillende landen door zelfde user dan nog kan dit verklaarbaar zijn. (AP Younes)
- Splunk bevat genoeg data voor de VPN (tot stuk in 2019), hopelijk ook genoeg firewall data
- Failover is uitgeschakeld

3.3 Te ondernemen acties

- Paswoord reset op sync accounts voor firewall en Infoblox. Proximus medewerker gevraagd ter ondersteuning (AP Aimad)
- Kijken in Splunk welke protocollen allemaal gebruikt worden (AP Younes)
- Na meeting gaat Younes de disk ophalen, deze wordt gecloned en teruggeplaatst.
- Vanaf donderdag cluster terug opbouwen voor failover

4 *<2020-08-07 Fri>* - Vervolg

4.1 Aanwezigen

Naam	Organisatie	Rol
Koen Colpaert	FenB	CISO
Maarten Massart	FenB	Netwerk
Aimad Soultanin	FenB	Netwerk
Peter Van den Neucker	FenB	CIO
Renaud Duois	HBplus	
Dirk Van Der Sanden	DXC	
Kurt Goris	Proximus	1I/ESE
Bart Cober	Proximus	1ITESE
Ward Bemelmans	FenB	Staf

4.2 Reeds ondernomen acties

- Status van de SSH key werd bekeken en bevestigd dat SSH toegang volledig disabled staat (ook voor admin)
- Session roaming staat uit zodat de cookies niet kunnen misbruikt worden
- Maarten heeft local users allemaal uitgeschakeld, dat blijkt gezien bovenstaande niet nodig maar gegeven de informatie waarover we beschikten de logische stap

4.3 Te ondernemen acties

- Alle local accounts moeten MFA enabled hebben
- Service accounts op AD en Radius moeten veranderd worden (2x op AD)
- Zijn dit priviliged accounts? Volgens Tom niet
- Alle PIN's voor non-local accounts resetten
- Failover naar passive mode ingepland op maandag als Younes groen licht heeft van Aimad dat de sync doorbroken is

Door bovenstaande acties en configuraites is het uit de lucht halen niet meer zo dringend. Eerst alle users aanpakken, logs bekin dan pas de disk

halen als er geen failover meer is. Aimad verwittigd Younes wanneer de sync uitstaat. Resetten van PIN blijkt niet geautomatiseerd te kunnen (mail config?), helpdesk gaat dat maandag persoon per persoon doen.

4.4 Communicatie

Maandag communicatie uitsturen naar alle gebruikers dat de PIN gaat gereset worden.

5 *<2020-08-07 Fri>*

5.1 Reeds ondernomen acties

- Proximus vroeg en kreeg goedkeuring voor CSIRT-offerte (3000€ opzetkost + 15000€ voor 10 mandagen)
- Eerste logs werden reeds doorgestuurd aan Younes

5.2 Bespreking

Uit een eerste analyse van de logs blijkt dat er maar een retentie is van 3 weken. Dit is een gevolg van onze upgrade van de versie in juli. De rest van de historiek zouden we uit Splunk moeten kunnen halen.

5.3 Te ondernemen acties

- Younes krijgt 3 logs (voor en na upgrade en huidige toestand)
- Failover wordt uitgezet
- Passief wordt standalone
- Alle linken op actieve omgeving uitschakelen
- Dump maken van configuratie profielen: weten wie toegang heeft tot wat (ook belangrijk voor de restore van de users)
- Younes krijgt een laptop van FB, een FB-profiel in AD met zelfde rechten als Aimad en lokale beheerdersrechten
- Toegang opzetten in Splunk voor Younes
- Uitsluitsel krijgen over SSH key: welke werd gelekt?

- Proximus bekijkt de mogelijkeden om Aimad extra ondersteuning te bieden

5.4 Open vragen

Hoe staat de session roaming ingesteld? Afhankelijk daarvan kan de cookie misbruikt zijn om aan te melden op andere omgevingen.

6 *<2020-08-06 Thu>*

6.1 Aanwezigen

Naam	Organisatie	Rol
Peter Van den Neucker	FenB	CIO
Koen Colpaert	FenB	CISO
Ward Bemelmans	FenB	Staf
Tom Janssens	FenB	Systemen
Bart Cober	Proximus	1IT/ESE
Wouter Godefroy	Proximus	1IT/ESE
Renaud Dubois	HBplus	DXC
Erik Hendrix	Proximus	SAL/STF
Younes Fourir	Proximus	GCA/SGI
Kurt Goris	Proximus	1IT/SSI
Aimad Soultani	FenB	Netwerk

6.2 Probleemstelling

Op Ruschische hackersfora doet een bestand de ronde met gehackte gegevens van de Pulse Secure omgevingen. Deze vulnerability werd door Pulse Secure opgemerkt op 24 april. FB heeft de bestaande systemen gepatched op 17 juli (doorlooptijd 85 dagen). Uit de gelekte gegevens van FB blijkt dat er een logbestand werd gedumpt met als laatste entry 24 juni. We moeten er dus van uitgaan dat er 1) toegang is geweest door onbevoegden tot deze omgeving en 2) dat dit gelopen heeft tot en met 24 juni (62 dagen). Door de patch is onze omgeving terug secure en de gebruikers accounts werken met MFA dus daar is ook nauwelijks risico. Uit forensisch onderzoek van de Pulse Secure omgeving moet blijken of er nog andere omgevingen bij deze hack betrokken zijn.

6.3 Bespreking

FB en Proximus bespreken samen de situatie op donderdag 6 augustus om de mogelijke risico's in te schatten en scenario's voor te stellen. Informatie over de vulnerability kan teruggevonden worden op Zdnet. Specifiek werd wereldwijd gebruik gemaakt van vulnerability CVE-2019-11510 (Unauthenticated remote attacker with network access via HTTPS can send a specially crafted URI to perform an arbitrary file reading vulnerability) om toegang te krijgen tot Pulse Secure omgevingen. Volgens de huidige informatie werden zo'n 900 systemen gecompromiteerd in de periode van 24 juni tot 8 juli 2020. Door deze exploitatie werden logs geëxporteerd.

De gelekte informatie voor onze omgeving bevat:

- Pulse Secure versie
- de Private SSH Key (start met "MIIEvgIBADANBg")
- gebruikersgegevens zoals username, user ID password hash en password
- log van de logingegevens (username, paswoord, IP adres, OS, MAC en laatste login)
- VPN coockie settings

Binnen FB maken we gelukkig gebruik van MFA waardoor slechts eenmalige paswoorden gelekt werden, enkel de eerste 4 cijfers (PIN) van de gebruikers paswoorden zijn dezelfde, de rest wordt gegenereerd door de VASCO tokens (app of hardware). Daardoor is het onmogelijk dat een hacker via deze gegevens verdere toegangen kon hebben aangezien die niet over de bedrijfseigen token beschikt. Dat is evenwel mogelijk door gebruik te maken van de lokale accounts (geen MFA) of de SSH key. Daarom is forensisch onderzoek van de omgeving door specialisten aangewezen.

De VPN omgeving wordt enkel gebruikt voor OOB dus gewone gebruikers zouden geen hinder mogen ondervinden van de uitschakeling.

6.4 Te nemen acties

- Pulse Secure uitschakelen:
  - de bestaande cluster wordt verbroken
  - actieve machine wordt afgekoppeld voor forensisch onderzoek
  - passieve machine wordt volledig van 0 terug opgebouwd, users worden 1 per 1 terug toegevoegd

  - Disabled users verdwijnen
  - Locked users moeten nieuwe credentials krijgen
  - Alle users krijgen een nieuwe PIN (er zijn 221 actieve users en 5 zijn gelocked)
  - MFA wordt de standaard, geen lokale gebruikers meer behalve lokale admin
  - Admin paswoord wordt aangepast
  - Nieuwe SSH key
  - Lijst maken van alle gebruikers zonder MFA in bestaande configuratie
- Alle users MOETEN over de laatse client + config beschikken, wie aanmeldt met een oude client vliegt er uuit
- Andere delen omgeving uitschakelen? Moet blijken uit forensisch onderzoek hoe ver de blootstelling reikt
- Proximus doet het nodige voor een CSIRT-contract voor FB

6.5 Communicatie

- Koen Algoed en David Van Herreweghe inlichten. Is gedaan door PVDN
- OOB gebruikers worden ingelicht door mail Liesbeth, tot zondagavond geen OOB toegang
- Helpdesk communiceert enkel wat door crisisteam werd goedgekeurd
- Melding maken in register?
- Nog geen communicatie naar buitenwereld

6.6 Open vragen

- Welke VLAN's zijn toegankelijk vanaf Pulse Secure?
- Heeft SSH nog andere toegangen?
- Zijn andere systemen gecompromiteerd en zo ja welke?