



## Rapportage Penetratietest DAK Kindercentra



11 maart 2025  
Strikt vertrouwelijk

---

YOUR SUCCESS SECURED

# Rapportage Penetratietest DAK Kindercentra

Vitaen biedt hoogwaardige consultancy op het gebied van fysieke beveiliging, cyberbeveiliging, compliance en risicomanagement. Onze diensten omvatten advies, auditing, interim management, incident- en crisismanagement en trainingen. We richten ons op zowel de private als publieke sector, waarbij we organisaties ondersteunen in het integreren van beveiliging en compliance binnen hun kernactiviteiten.

Opdrachtgever  
DAK Kindercentra

Datum  
11 maart 2025

Documentnummer  
20250309.DAK.1.0

Versie  
V.1.0

Auteurs  
De heer R. Dijkstra

Vitaen BV  
Regulusweg 5 (6e etage)  
2516 AC Den Haag  
KVK 74284932  
[www.vitaen.nl](http://www.vitaen.nl)



# Inhoudsopgave

---

<b>Management Samenvatting.....</b>	<b>4</b>
Scopebeschrijving.....	4
Overzicht bevindingen .....	5
<b>Inleiding .....</b>	<b>6</b>
Doel.....	6
Scopebeschrijving.....	6
Beperkingen .....	6
<b>Aanpak .....</b>	<b>7</b>
Common Vulnerability Scoring System .....	7
Risico classificatie bevindingen .....	9
<b>Bevindingen .....</b>	<b>10</b>
Onderzoek bevindingen .....	<b>Error! Bookmark not defined.</b>
ID: F.11 – Kerberoastable Domain Admin Account .....	11
ID: F.8 – Service Accounts with domain admin rechten .....	13
ID: F.1 – WP-Cron.php Beschikbaar .....	14
ID: F.3 – Users.json beschikbaar voor anonieme gebruikers .....	15
ID: F.4 – Toegang tot xml-rpc.php voor anonieme gebruikers .....	17
ID: F.10 – Kerberoastable service accounts .....	19
ID: F.12 – Lokale webapplicatie draaiend op port 80 .....	20
ID: F.2 – DMARC: Quarantine/Reject policy niet geconfigureerd.....	21
ID: F.5 – Missende security headers.....	22
ID: F.6 – Default Admin account actief binnen Azure .....	24
ID: F.7 – Applicatiegeheim met te lange einddatum .....	26
ID: F.9 – Verouderde Servers .....	28



# Management Samenvatting

Dit rapport is het resultaat van een cybersecurity assessment uitgevoerd door Vitaen B.V. in de periode 3 maart t/m 7 maart 2025 voor DAK Kindercentra.

Gedurende dit security assessment is de navolgende aanpak uitgevoerd.

- **Blackbox**, zonder gegevens vooraf verkregen
  - Geautomatiseerde web applicatie scan
  - Handmatige verificatie van de geautomatiseerde web applicatie scan
  - Handmatige web applicatie test
  - Vulnerability scan infrastructuur
  - Handmatige verificatie van de vulnerability scan infrastructuur
  - Handmatige infrastructuur test (indien van toepassing ter aanvulling op het onderzoek.)
- **Graybox**, met basis toegangsrechten
  - Vulnerability scan infrastructuur
  - Handmatige verificatie van de vulnerability scan infrastructuur
  - Handmatige infrastructuur test (indien van toepassing ter aanvulling op het onderzoek.)

De componenten hieronder in de scopebeschrijving vermeld, zijn onderzocht op kwetsbaarheden in de cyberbeveiliging die kunnen leiden tot verlies van vertrouwelijkheid, integriteit of beschikbaarheid.

## Scopebeschrijving

Voor dit security assessment vallen de volgende domeinnamen, ip-adressen, hostnamen en rollen binnen de scope zoals vastgesteld in "Security Testplan DAK 2025-2 V1.0"

### Scope onderzoek

Productieomgeving:

- Locatie kinderdagverblijf (Lamgroen 18, 2511 XE Den Haag)
- Locatie Servicekantoor (Maanweg 174, 2516 AB Den Haag)
- Azure omgeving
- Externe componenten DAK

Het doel van deze security assessments is als volgt gedefinieerd:

Inzicht te krijgen in de effectiviteit van de getroffen beveiligingsmaatregelen, de weerstand van de infrastructuur en in welke mate deze omgeving vatbaar is voor een succesvolle aanval door een hacker of kwaadwillend persoon.

## Overzicht bevindingen

Identificatie nummer	Naam bevinding	Risicoclassificatie
ID: F.11	Kerberoastable Domain Admin Account	Hoog
ID: F.1	WP-Cron beschikbaar	Medium
ID: F.8	Service Accounts met domain admin rechten	Medium
ID: F.3	Users.json beschikbaar voor anonieme gebruikers	Laag
ID: F.4	Toegang tot xml-rpc.php voor anonieme gebruikers	Laag
ID: F.10	Kerberoastable service accounts	Laag
ID: F.12	Web applicatie draaiend op port 80	Laag
ID: F.2	DMARC: Quarantine/Reject policy niet geconfigureerd	Informatief
ID: F.5	Missende security headers	Informatief
ID: F.6	Default Admin account actief binnen Azure	Informatief
ID: F.7	Applicatiegeheim met te lange einddatum	Informatief
ID: F.9	Verouderde Servers	Informatief

De locatiebezoeken hebben geen grote of onverwachte risico's aan het licht gebracht. De algemene beveiligingsstatus is goed. Desalniettemin is er ruimte voor verbetering. Er zijn enkele kwetsbaarheden geïdentificeerd die mogelijk impact kunnen hebben op de veiligheid. Momenteel heeft het veelal te maken met oude configuratie die, tijdens gesprekken op de wandelgangen, al van te voren deels bekend waren en mogelijk moeilijk te mitigeren. Toch is het belangrijk deze tijdens deze pentest alsnog te benoemen, om in ieder geval ook een direct risico er aan te koppelen.

# Inleiding

---

Vitaen heeft een beveiliging beoordelingsonderzoek (security assessment) uitgevoerd op de externe omgeving van Dak Kindercentra waarbij de technische beveiligingsmaatregelen zijn getest op aanwezige digitale kwetsbaarheden.

De bevindingen van dit rapport zijn het resultaat van een blackbox penetratietest onderzoek welke extern is uitgevoerd. Deze test is uitgevoerd in de periode van 3 maart t/m 7 maart 2025.

De in scope vermelde onderdelen zijn onderzocht op kwetsbaarheden die kunnen leiden tot verstoring van de betrouwbaarheid (vertrouwelijkheid, integriteit en beschikbaarheid). De resultaten van deze testen, en de aanbevelingen ter verbetering, zijn opgenomen in deze rapportage.

## Doel

Het doel van deze security assessment is als volgt gedefinieerd:

Het testen van de effectiviteit van de getroffen beveiligingsmaatregelen, de weerstand van de infrastructuur en in welke mate de omgeving vatbaar is voor een succesvolle aanval door een kwaadwillend persoon of organisatie.

## Scopebeschrijving

Voor dit security assessment vallen de volgende domeinnamen, ip-adressen, hostnamen en rollen binnen de scope zoals vastgesteld in "Security Testplan DAK 2025-2 V1.0"

### Scope onderzoek

Productieomgeving:

- Locatie kinderdagverblijf (Lamgroen 18, 2511 XE Den Haag)
- Locatie Servicekantoor (Maanweg 174, 2516 AB Den Haag)
- Azure omgeving
- Externe componenten DAK

## Beperkingen

Met behulp van dit security assessment kan alleen worden aangetoond of het mogelijk is de beveiligingsmaatregelen te doorbreken. Er kan niet met zekerheid worden gesteld dat geïmplementeerde beveiligingsmaatregelen niet doorbroken kan worden. Een aanvaller met ongelimiteerd budget, kennis en tijd zal vrijwel altijd slagen in het doorbreken van de beveiliging. Vitaen heeft deze security test uitgevoerd met een optimale verhouding tussen budget en in/output.

Vitaen heeft geen zogenaamde 'denial-of-service' of 'social-engineering- technieken' toegepast. Denial-of-service is het onbereikbaar maken van de te leveren diensten. Social-engineering is het achterhalen van persoonlijke informatie door onderzoek op internet, social-media en/of door persoonlijke contact te leggen.



Enkel op basis van de uitkomsten van het onderzoek, kan geen conclusie over het niveau van het totaalbeeld van de beveiliging worden gegeven. Immers, een adequate beveiliging omvat niet alleen technische maar ook, bouwkundige en organisatorisch maatregelen waarbij opzet bestaan en werking in lijn moeten zijn met het vastgestelde risicoprofiel.

Er kan geen gebruik gemaakt worden van aanvallen op kwetsbaarheden die niet publiekelijk bekend zijn, zogenaamde zero-day aanvallen.

## Aanpak

In een security assessment genereert en verstuurt Vitaen ongeautoriseerde en ongewenste invoer naar systemen om de effectiviteit van bestaande beveiligingsmaatregelen te testen. Voor Vitaen betekent een security assessment meer dan alleen het uitvoeren van een scan met standaard, geautomatiseerde programmatuur. Wij voeren ook handmatige scans uit om kwetsbaarheden op te sporen die door standaard software worden gemist. Daarnaast analyseren en verifiëren we zorgvuldig de geconstateerde zwakheden om de correctheid en impact ervan te beoordelen.

Vitaen voert security assessments uit volgens erkende richtlijnen en standaarden, afhankelijk van de specifieke situatie.

- OWASP Application Security Verification Standard <https://owasp.org/www-project-application-security-verification-standard/>
- OWASP API Security Project <https://owasp.org/www-project-api-security/>
- OWASP Secure Headers Project <https://owasp.org/www-project-secure-headers>
- NCSC-NL - ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) <https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1>
- MITRE ATT&CK® Matrix for Enterprise [MITRE ATT&CK®](#)
- The Open Source Security Testing Methodology [OSSTMM 3](#)
- Penetration Testing Execution Standard (PTES) [The Penetration Testing Execution Standard](#)
- NIST Technical Guide to Information Security Testing and Assessment [NIST Special Publication \(SP\) 800-115, Technical Guide to Information Security Testing and Assessment](#)

## Common Vulnerability Scoring System

Kwetsbaarheden tijdens dit onderzoek gevonden, worden ingeschat volgens het Common Vulnerability Scoring System (CVSS versie 3.x). CVSS is een open raamwerk voor het communiceren van kenmerken en de ernst van software kwetsbaarheden. Vitaen gebruikt dit raamwerk om de ernst te berekenen van

kwetsbaarheden die in de digitale omgeving zijn ontdekt in het kader van de beoordeling en als factor bij prioriteren van herstelactiviteiten voor kwetsbaarheden.

### Vector string

De CVSS vector string is een tekstweergave van een set CVSS-statistieken. Het wordt vaak gebruikt om CVSS-metrische informatie in een beknopte vorm vast te leggen of over te dragen. CVSS is een gepubliceerde standaard die door organisaties over de hele wereld wordt gebruikt. Meer hierover is te vinden op: <https://nvd.nist.gov/vuln-metrics/cvss>.

### Kwalitatieve beoordelingsschaal

Onderstaand tabel geeft tekstuele weergave van de numerieke basis-, temporele en omgeving scores zoals gedefinieerd volgens CVSS richtlijnen.

Beoordeling	CVSS Score
Kritiek	9.0 - 10.0
Hoog	7.0 - 8.9
Medium	4.0 - 6.9
Laag	0.1 - 3.9
Geen	0.0

Tabel: CVSS v3



## Risico classificatie bevindingen

Dit hoofdstuk bevat een gedetailleerde beschrijving van de geconstateerde bevindingen en onze aanbevelingen.

RISICOCLASSIFICATIE	
KRITIEK	<b>Kritiek risico:</b> Een risico dat als 'kritiek' is geclassificeerd, vormt een directe bedreiging voor de continuïteit van de informatievoorziening, de IT-infrastructuur en/of de applicatie. De uitvoer van de mitigatie is niet complex, maar de impact is zeer groot.
HOOG	<b>Hoog risico:</b> Een 'hoog' geclassificeerd risico kan een serieuze bedreiging vormen voor de continuïteit van de informatievoorziening, de IT-infrastructuur en/of de applicatie. Dit risico kan direct leiden tot ongeautoriseerde toegang of ongeautoriseerd gebruik van onderdelen van deze systemen.
GEMIDDELD	<b>Gemiddeld risico:</b> Een risico met de classificatie 'gemiddeld' kan het functioneren van de informatievoorziening, de IT-infrastructuur en/of de applicatie verstoren. Het kan indirect leiden tot ongeautoriseerde toegang of ongeautoriseerd gebruik. Dit risico wijst vaak op onvoldedige beveiligingsmaatregelen en impliceert een verhoogde kans dat op termijn een hoog risico ontstaat.
LAAG	<b>Laag risico:</b> Een risico dat als 'laag' is geclassificeerd, kan een kleine verstoring veroorzaken, maar zal niet direct leiden tot ongeautoriseerde toegang of ongeautoriseerd gebruik van componenten binnen de informatievoorziening, de IT-infrastructuur en/of de applicatie.
INFORMATIEF	<b>Informatief risico:</b> Een als 'informatief' geclassificeerd risico veroorzaakt geen verstoring, maar wordt gemeld om mogelijke verbeteringen of optimalisaties in de beveiliging aan te bevelen.

In de bevindingen tabel zijn de bevindingen en aanbevelingen beschreven. In de tabel zijn de volgende kolommen opgenomen:

1. ID: iedere bevinding heeft een eigen nummer.
2. Common Vulnerability Scoring System (CVSSv3) score
3. Beschrijving van de kwetsbaarheid of het risico
4. Reproductiestappen van de bevinding
5. Impact beschrijving of risico van de bevinding
6. Oplossingsrichting bevinding of te nemen mitigerende maatregelen bij het risico.
7. Scope object
8. Risico bepaling

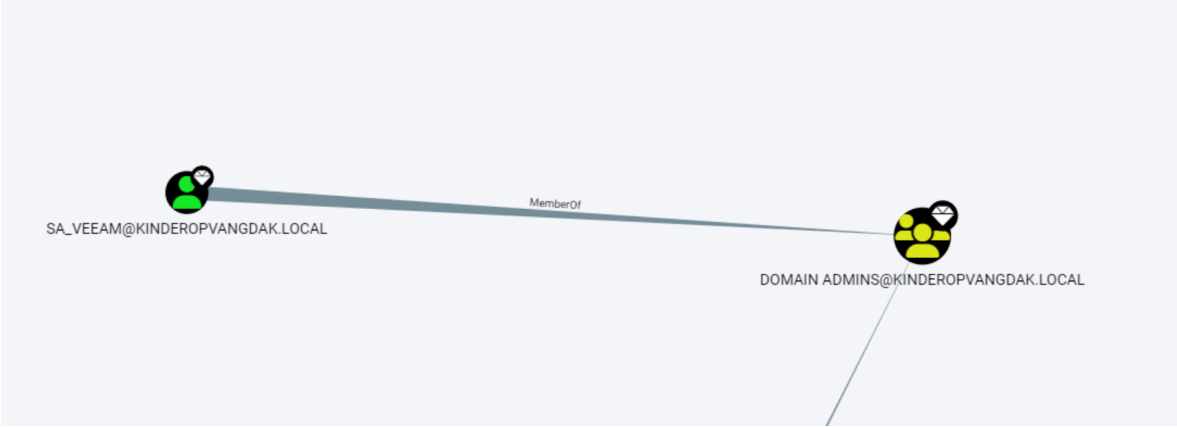
De bevindingen worden weergegeven op basis van een risico inschatting. De eerstgenoemde bevindingen lopen het meest risico en de laatstgenoemde het minst. Ter verhoging van de leesbaarheid worden velden toegevoegd of verwijderd waar nodig.

## Bevindingen

Identificatie nummer	Naam bevinding	Risicoclassificatie
ID: F.11	Kerberoastable Domain Admin Account	Hoog
ID: F.1	WP-Cron beschikbaar	Medium
ID: F.8	Service Accounts met domain admin rechten	Medium
ID: F.3	Users.json beschikbaar voor anonieme gebruikers	Laag
ID: F.4	Toegang tot xml-rpc.php voor anonieme gebruikers	Laag
ID: F.10	Kerberoastable service accounts	Laag
ID: F.12	Web applicatie draaiend op port 80	Laag
ID: F.2	DMARC: Quarantine/Reject policy niet geconfigureerd	Informatief
ID: F.5	Missende security headers	Informatief
ID: F.6	Default Admin account actief binnen Azure	Informatief
ID: F.7	Applicatiegeheim met te lange einddatum	Informatief
ID: F.9	Verouderde Servers	Informatief



## ID: F.11 – Kerberoastable Domain Admin Account

<b>RISICOCLASSIFICATIE</b> <b>Hoog</b>
<b>CVSS score: CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H</b>
<b>Owasp category: A04:2021 – Insecure Design</b>
<p><b><u>Beschrijving van de kwetsbaarheid of het risico</u></b></p> <p>Tijdens het onderzoek is vastgesteld dat het account SA_VEEAM beschikt over Domain Administrator-rechten. Dit brengt een verhoogd risico met zich mee, aangezien een compromis van dit account directe toegang geeft tot de volledige Active Directory-omgeving. Accounts met dergelijke rechten vormen een aantrekkelijk doelwit voor aanvallers en moeten met extra zorg worden beheerd.</p> <p>Het gebruik van een service account met Domain Admin-rechten is in de meeste gevallen niet noodzakelijk en verhoogt het aanvalsoppervlak aanzienlijk. Dit geldt met name voor back-upsoftware zoals Veeam, waarbij het principe van least privilege zou moeten worden toegepast. Een aanvalleur die dit account weet te compromitteren, kan back-ups manipuleren, verwijderen of zelfs de volledige Active Directory overnemen. Aangezien dit account vatbaar is voor een Kerberoasting aanval, is het mogelijk gebleken de wachtwoord hash te bemachtigen. Het bleek echter niet mogelijk in de korte tijd dat de opdracht plaatsvond, om hiervan het wachtwoord te brute-forcen. Echter, met genoeg tijd en resources zou dit zeker mogelijk zijn.</p>  <pre>graph LR; SA_VEEAM@KINDEROPVANGDAK.LOCAL -- MemberOf --&gt; DOMAIN_ADMINS@KINDEROPVANGDAK.LOCAL</pre> <p><b><u>Oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen</u></b></p> <p>Vitaen adviseert om:</p> <ul style="list-style-type: none"><li>De rechten van SA_VEEAM te herzien en te minimaliseren. In de meeste gevallen heeft Veeam geen Domain Admin-rechten nodig, maar slechts specifieke rechten op de systemen die het beheert.</li></ul>

- Een apart account voor Veeam-back-ups aan te maken met alleen de noodzakelijke permissies, zonder lidmaatschap van de Domain Admins-groep.
- Regelmatige monitoring en logging van het account in te stellen, zodat afwijkend gedrag zoals ongebruikelijke aanmeldingen of bewerkingen snel worden gedetecteerd.

**Locatie van de kwetsbaarheid:**

DAK Active Directory

**Score: 7.1**

## ID: F.8 – Service Accounts with domain admin rechten

<b>RISICOCLASSIFICATIE</b> <b>Medium</b>
<b>CVSS score: CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N</b>
<b>Owasp category: A04:2021 – Insecure Design</b>
<p><b><u>Beschrijving van de kwetsbaarheid of het risico</u></b></p> <p>Tijdens de controle is vastgesteld dat meerdere service accounts over Domain Admin-rechten beschikken. Hoewel service accounts bedoeld zijn voor geautomatiseerde taken en applicaties, brengt het toekennen van dergelijke hoge privileges aanzienlijke risico's met zich mee.</p> <p>Service accounts worden vaak gebruikt door meerdere systemen en processen, waardoor ze minder goed beheerd worden dan reguliere gebruikersaccounts. In combinatie met Domain Admin-rechten betekent dit dat een aanvaller, bij compromittering van dit account, volledige controle over de Active Directory kan verkrijgen. Dit opent de deur naar privilege escalation, laterale beweging binnen het netwerk en zelfs volledige overname van de IT-infrastructuur. Bovendien worden service accounts vaak uitgesloten van multi-factor authenticatie (MFA), wat het risico op misbruik verder vergroot.</p> <p>Het gaat om de volgende service accounts:</p> <ul style="list-style-type: none"><li>• SA_CITRIX@KINDEROPVANGDAK.LOCAL</li><li>• SA_VEEAM@KINDEROPVANGDAK.LOCAL</li><li>• SA_KOCON@KINDEROPVANGDAK.LOCAL</li><li>• SA_AVENSUS@KINDEROPVANGDAK.LOCAL</li><li>• SA_PRTG@KINDEROPVANGDAK.LOCAL</li><li>• SA_VC@KINDEROPVANGDAK.LOCAL</li></ul>
<p><b><u>Oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen</u></b></p> <p>Vitaen adviseert om het principe van least privilege toe te passen: service accounts mogen alleen de rechten krijgen die strikt noodzakelijk zijn voor hun functionaliteit. Waar mogelijk moeten alternatieve oplossingen zoals Managed Service Accounts (MSA) of Group Managed Service Accounts (gMSA) worden gebruikt, die automatisch wachtwoorden roteren en minder risicovol zijn. Daarnaast moet het gebruik van service accounts met verhoogde rechten actief worden gemonitord en gelogd, zodat afwijkend gedrag direct wordt opgemerkt.</p>
<p><b>Locatie van de kwetsbaarheid:</b> DAK Active Directory</p>
<b>Score: 6.4</b>

## ID: F.1 – WP-Cron.php Beschikbaar

<b>RISICOCLASSIFICATIE</b> <b>Medium</b>	
<b>CVSS score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L</b>	
<b>Owasp category: A05:2021 – Security Misconfiguration</b>	
<p><b>Beschrijving van de kwetsbaarheid of het risico</b></p> <p>De WordPress WP-Cron.php endpoint is publiekelijk toegankelijk, wat aanvallers in staat stelt om ongeautoriseerde cron-taken uit te voeren of herhaaldelijk cron-verzoeken te sturen. Dit kan de prestaties van de server beïnvloeden door overmatig gebruik van systeembronnen, wat resulteert in een Denial-of-Service (DoS)-aanval. WP-Cron.php is een virtueel cron systeem dat wordt gebruikt door WordPress om geplande taken uit te voeren, maar het is niet ontworpen om openbaar toegankelijk te zijn voor anonieme gebruikers.</p> <p><b>Reproductie pad:</b></p> <p>Voer de onderstaande URL in de browser in.</p> <div>https://www.dakkindercentra.nl/wp/wp-cron.php</div> <p><b>HTTP response</b></p> <div>HTTP/2 200 OK Server: openresty Date: Thu, 13 Mar 2025 12:49:11 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Vary: Accept-Encoding Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Age: 0 X-Varnish-Cache: MISS Accept-Ranges: bytes Swlh: 1</div> <p><b>Oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen:</b></p> <p>Vitaen adviseert om de toegang tot WP-Cron.php door middel van IP-restricties of authenticatie te beperken. Alternatief kan WP-Cron.php uitgeschakeld worden in de WordPress-configuratie (wp-config.php) en vervangen worden door de server-gebaseerde cron om geplande taken uit te voeren. Dit voorkomt ongewenste toegang en minimaliseert de kans op misbruik.</p> <p><b>Locatie van de kwetsbaarheid</b></p> <p>Dakkindercentra.nl</p> <tr><td><b>Score: 5.3</b></td></tr>	<b>Score: 5.3</b>
<b>Score: 5.3</b>	

## ID: F.3 – Users.json beschikbaar voor anonieme gebruikers

<b>RISICOCLASSIFICATIE</b> <b>Laag</b>
<b>CVSS score: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O</b>
<b>Owasp category: A05:2021 – Security Misconfiguration</b>
<p><b>Beschrijving van de kwetsbaarheid of het risico:</b></p> <p>Het bestand users.json werd gevonden op de webapplicatie, waardoor gevoelige informatie over de gebruikers van het WordPress-platform zichtbaar is. Deze informatie kan misbruikt worden door aanvallers om inloggegevens te brute-forcen of gebruikersaccounts te manipuleren.</p> <p><b>HTTP Request</b></p> <pre>GET /wp-json/wp/v2/users HTTP/1.1 Host: www.dakkindercentra.nl Accept-Encoding: gzip, deflate Accept: */* Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.127 Safari/537.36 Connection: close</pre> <p>Voorbeeld boven: HTTP verzoek verstuurd naar de server</p> <p><b>HTTP Response</b></p> <pre>HTTP/2 200 OK Server: openresty Date: Thu, 13 Mar 2025 12:49:58 GMT Content-Type: application/json; charset=UTF-8 Content-Length: 4045 Vary: Accept-Encoding, Origin X-Robots-Tag: noindex Link: &lt;https://www.dakkindercentra.nl/wp-json/&gt;; rel="https://api.w.org/" X-Content-Type-Options: nosniff Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link Access-Control-Allow-Headers: Authorization, X-WP-Nonce, Content-Disposition, Content-MD5, Content-Type X-Wp-Total: 6 X-Wp-Totalpages: 1 Allow: GET Age: 0 X-Varnish-Cache: MISS Accept-Ranges: bytes Swlh: 1  [{"id":16,"name":"Charo van Eijk","url":"","description":"","link":"https://www.dakkindercentra.nl/autho</pre>

```
r\charo\/","slug":"charo","avatar_urls":{"24":"https://secure.gravatar.com/avatar/d781131544db66dc32d85e6065b1b514?s=24&d=mm&r=g","48":"https://secure.gravatar.com/avatar/d781131544db66dc32d85e6065b1b514?s=48&d=mm&r=g","96":"https://secure.gravatar.com/avatar/d781131544db66dc32d85e6065b1b514?s=96&d=mm&r=g"},"meta":[],"acf":[],"_links":{"self":[{"href":"https://www.dakkindercentra.nl/wp-json/wp/v2/users/16","targetHints":{"allow":["GET"]}}],"collection":[{"href":"https://www.dakkindercentra.nl/wp-json/wp/v2/users"}]}},{ "id":19,"name":"Iris Obdeijn",
[...]
```

Voorbeeld boven: HTTP response ontvangen van de server met hierin de gegevens van de Wordpress gebruikers (aangepast voor leesbaarheid)

#### Reproductie pad:

Voer de onderstaande URL in de browser in.

```
https://www.dakkindercentra.nl/wp-json/wp/v2/users
```

#### Oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen:

Vitaen adviseert om de toegang tot de wp-users.json endpoint af te schermen door deze alleen beschikbaar te maken voor geauthenticeerde en geautoriseerde gebruikers. Overweeg ook om gebruikersnamen te maskeren of de informatie die via deze API wordt verstrekt te beperken, zodat alleen noodzakelijke gegevens worden gedeeld

#### Locatie van de kwetsbaarheid:

Dakkindercentra.nl

**Score: 3.7**



## ID: F.4 - Toegang tot xml-rpc.php voor anonieme gebruikers

<b>RISICOCLASSIFICATIE</b> <b>Laag</b>
<b>CVSS score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N</b>
<b>Owasp category: A05:2021 – Security Misconfiguration</b>
<p><b>Beschrijving van de kwetsbaarheid of het risico:</b></p> <p>Het bestand xml-rpc.php is toegankelijk voor niet-geauthenticeerde gebruikers, wat potentieel kan leiden tot brute-force aanvallen en Denial of Service (DoS)-aanvallen. De XML-RPC-interface in WordPress biedt functionaliteit waarmee externe services kunnen communiceren met de website, zoals publiceren van posts op afstand. Echter, deze functionaliteit kan worden misbruikt door aanvallers om bijvoorbeeld een grote hoeveelheid loginpogingen in één verzoek te versturen of om de server te overbelasten via DoS-aanvallen.</p> <p><b>Reproductie pad:</b></p> <p>Voer de onderstaande URL in de browser in.</p> <div><a href="https://www.dakkindercentra.nl/wp/xmlrpc.php">https://www.dakkindercentra.nl/wp/xmlrpc.php</a></div> <p><b>HTTP GET request</b></p> <div><pre>POST /xmlrpc.php HTTP/2 Host: www.dakkindercentra.nl Cookie: _gid=GA1.2.1724863973.1740390034; [...] Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Priority: u=0, i Content-Length: 91  &lt;methodCall&gt; &lt;methodName&gt;system.listMethods&lt;/methodName&gt; &lt;params&gt;&lt;/params&gt; &lt;/methodCall&gt;</pre></div> <p><b>HTTP response</b></p> <div><pre>HTTP/2 200 OK Server: openresty Date: Thu, 13 Mar 2025 12:51:25 GMT Content-Type: text/xml; charset=UTF-8 Content-Length: 4272</pre></div>

```
Vary: Accept-Encoding
Age: 0
X-Varnish-Cache: MISS
Accept-Ranges: bytes
Swlh: 1

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <params>
    <param>
      <value>
        <array><data>
          <value><string>system.multicall [...]
```

#### Oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen

Vitaen adviseert om de toegang tot xml-rpc.php uit te zetten als deze functionaliteit niet expliciet nodig is voor de werking van de website. Dit kan eenvoudig worden gedaan door de toegang tot het bestand te blokkeren via de serverconfiguratie of door een WordPress-plugin te gebruiken. Als XML-RPC-functionaliteit wel nodig is, overweeg dan het gebruik van alternatieven zoals de REST API, die veiliger kan worden geconfigureerd.

#### Locatie van de kwetsbaarheid

dakkindercentra.nl

**Score: 3.7**

## ID: F.10 – Kerberoastable service accounts

<b>RISICOCLASSIFICATIE</b> <b>Laag</b>
<b>CVSS score: CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N</b>
<b>Owasp category: A05:2021 – Security Misconfiguration</b>
<p><b><u>Beschrijving van de kwetsbaarheid of het risico</u></b></p> <p>Tijdens de audit is vastgesteld dat er service accounts aanwezig zijn die kwetsbaar zijn voor een Kerberoasting-aanval. Dit betekent dat de bijbehorende Kerberos Service Tickets kunnen worden opgevraagd en offline gekraakt om de wachtwoorden te achterhalen. Hoewel er wachtwoordkrakingspogingen zijn uitgevoerd zonder succes, blijft het risico bestaan dat met voldoende tijd en rekenkracht de wachtwoorden in de toekomst kunnen worden achterhaald.</p> <p>Kerberoasting is een bekende aanvalstechniek waarbij aanvallers gebruikmaken van zwakke encryptie in Kerberos Service Tickets, vooral als de wachtwoorden van service accounts niet complex genoeg zijn of lange tijd ongewijzigd blijven. Een succesvol gekraakt wachtwoord kan leiden tot verhoogde privileges binnen het domein en potentieel volledige compromittering van de omgeving.</p> <p>Tijdens de test, zijn de kerberos hashes van 3 account gecompromitteerd:</p> <ul style="list-style-type: none"><li>• Administrator</li><li>• SA_PVS</li><li>• Sa_veaam</li></ul> <p>Uit de analyse blijkt dat verschillende andere accounts, mogelijk ook nog kwetsbaar zijn voor deze aanval:</p> <ul style="list-style-type: none"><li>• SA_ADFS\$</li><li>• KRBTGT</li></ul>
<p><b><u>Oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen</u></b></p> <p>Vitaen adviseert om sterke, lange wachtwoorden te gebruiken voor service accounts (bij voorkeur minimaal 25 tekens) en regelmatig wachtwoordrotatie toe te passen. Daarnaast kan het gebruik van Group Managed Service Accounts (gMSA) helpen om dit type aanval te voorkomen, omdat deze accounts automatisch en veilig door Windows worden beheerd zonder statische wachtwoorden. Het beperken van service accountrechten tot het minimaal noodzakelijke en het monitoren van Kerberos-verzoeken op verdachte activiteiten kan verdere risico's verkleinen.</p>
<p><b>Locatie van de kwetsbaarheid:</b></p> <p>DAK Active Directory</p>
<b>Score: 3.7</b>

## ID: F.12 – Lokale webapplicatie draaiend op port 80

<b>RISICOCLASSIFICATIE</b> <b>Laag</b>
<b>CVSS score: CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N</b>
<b>Owasp category: A02:2021 – Cryptographic Failures</b>
<p><b><u>Beschrijving van de kwetsbaarheid of het risico</u></b></p> <p>Tijdens het onderzoek is vastgesteld dat een webapplicatie binnen het lokale netwerk draait op poort 80, zonder enige vorm van versleuteling. Dit betekent dat alle communicatie met de applicatie, inclusief eventuele inloggegevens of andere gevoelige informatie, onversleuteld wordt verzonden en daardoor kwetsbaar is voor afluisteren binnen het netwerk.</p> <p>Hoewel de applicatie niet direct vanaf het internet toegankelijk is, blijft het risico aanwezig. Binnen een intern netwerk kunnen kwaadwillenden of gecompromitteerde systemen netwerkverkeer onderscheppen via technieken zoals Man-in-the-Middle (MitM)-aanvallen. Dit kan ertoe leiden dat gevoelige informatie wordt buitgemaakt of dat sessies worden overgenomen.</p>
<p><b><u>Oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen</u></b></p> <p>Vitaen adviseert om:</p> <ul style="list-style-type: none"><li>• HTTPS (TLS) te implementeren, zodat alle communicatie met de applicatie versleuteld wordt. Dit kan eenvoudig worden gedaan met een lokaal gegenereerd certificaat of een certificaat van een interne CA.</li><li>• HTTP-verkeer automatisch door te sturen naar HTTPS, zodat gebruikers niet per ongeluk een onversleutelde verbinding gebruiken.</li><li>• De configuratie van de webserver te controleren, om te verzekeren dat alleen veilige versleutelingsprotocollen en cipher suites worden ondersteund.</li><li>• Netwerksegmentatie en toegangscontrole toe te passen, zodat alleen geautoriseerde systemen toegang hebben tot de applicatie.</li></ul>
<p><b>Locatie van de kwetsbaarheid:</b></p> <p>Kinderdagopvang locatie: 192.168.122.31</p>
<b>Score: 3.7</b>

## ID: F.2 – DMARC: Quarantine/Reject policy niet geconfigureerd

<b>RISICOCLASSIFICATIE</b> <b>INFORMATIEF - Geen risico</b>
<b>CVSS score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N</b>
<b>Owasp category: A05:2021 – Security Misconfiguration</b>
<p><b>Beschrijving van de kwetsbaarheid of het risico</b></p> <p>DMARC (Domain-based Message Authentication, Reporting &amp; Conformance) is een e-mailauthenticatieprotocol dat helpt bij het voorkomen van e-mailspoofing en phishingaanvallen. Wanneer een organisatie DMARC implementeert, kan het een beleid instellen om verdachte e-mails te behandelen, zoals "none," "quarantine," of "reject." Bij deze finding is geconstateerd dat er geen quarantine of reject beleid is ingesteld in de DMARC-records van het domein. Dit betekent dat e-mails die mogelijk spoofed of vervalst zijn, geen strikte behandeling krijgen en mogelijk toch in de inbox van de ontvanger terechtkomen.</p> <p><b>Risico:</b> Het niet instellen van een quarantine of reject beleid maakt het domein kwetsbaar voor misbruik door aanvallers die e-mails kunnen vervalsen (spoofing) en deze naar externe ontvangers sturen. Dit vergroot de kans op phishing-aanvallen, waarbij aanvallers proberen gevoelige informatie van gebruikers of medewerkers te verkrijgen. Het niet hebben van een strengere DMARC-beveiliging verhoogt de kans dat aanvallers succesvolle phishingcampagnes kunnen uitvoeren met het imiteren van het domein van de organisatie.</p> <p>Het huidige DMARC beleid is het volgende:</p> <pre>v=DMARC1; p=none; rua=mailto:bsyu7751wj@rua.powerdmarc.com; ruf=mailto:bsyu7751wj@ruf.powerdmarc.com; fo=1;</pre>
<p><b>Oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen</b></p> <p>Vitaen adviseert om het DMARC-beleid te configureren met een <b>quarantine</b> of <b>reject</b> instelling, afhankelijk van de organisatiebehoefte. Het <b>quarantine</b> beleid zorgt ervoor dat verdachte e-mails in de spamfolder terechtkomen, terwijl het <b>reject</b> beleid e-mails van verdachte afzenders volledig blokkeert. Begin met het instellen van <b>quarantine</b> om het effect te testen en verhoog daarna naar <b>reject</b> zodra je vertrouwen hebt in de werking van het systeem. Dit helpt om het risico op e-mailgerelateerde aanvallen te minimaliseren en de e-mailbeveiliging te versterken.</p>
<p><b>Locatie van de kwetsbaarheid</b></p> <p>dakkindercentra.nl</p>
<p><b>Score: 0</b></p>

## ID: F.5 – Missende security headers

<b>RISICOCLASSIFICATIE</b> <b>INFORMATIEF - Geen risico</b>
<b>CVSS score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N</b>
<b>Owasp category: A05:2021 – Security Misconfiguration</b>
<p><b>Beschrijving van de kwetsbaarheid of het risico</b></p> <p>De applicatie mist essentiële beveiligingsheaders die nodig zijn om bescherming te bieden tegen veelvoorkomende webaanvallen zoals Cross-Site Scripting (XSS), clickjacking, en man-in-the-middle aanvallen. Headers zoals Content-Security-Policy (CSP), X-Content-Type-Options en X-Frame-Options &amp; Strict-Transport-Security-Header missen in de HTTP-responses. Zonder deze headers is de applicatie kwetsbaarder voor deze aanvallen, wat de veiligheid van gebruikers en gegevens in gevaar brengt.</p> <p><b>Reproductie pad:</b></p> <p>Voer de onderstaande URL in de browser in.</p> <div data-bbox="215 1019 606 1050"> <a href="https://www.dakkindercentra.nl/">https://www.dakkindercentra.nl/</a> </div> <p><b>HTTP response</b></p> <pre> HTTP/2 200 OK Server: openresty Date: Thu, 13 Mar 2025 12:48:27 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 115564 Vary: Accept-Encoding Link: &lt;https://www.dakkindercentra.nl/wp-json/&gt;; rel="https://api.w.org/" Link: &lt;https://www.dakkindercentra.nl/wp-json/wp/v2/pages/5&gt;; rel="alternate"; title="JSON"; type="application/json" Link: &lt;https://www.dakkindercentra.nl/&gt;; rel=shortlink Age: 4349 X-Varnish-Cache: HIT Accept-Ranges: bytes Swlh: 1 </pre>
<p><b>Oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen</b></p> <p>Vitaen adviseert om de ontbrekende beveiligingsheaders toe te voegen aan de serverconfiguratie. Gebruik Content-Security-Policy (CSP) om de bronnen die op de website geladen kunnen worden te beperken, X-Content-Type-Options om MIME-type sniffing te voorkomen, X-Frame-Options om clickjacking tegen te gaan. Strict-transport-Security om SSL te forceren. Zorg ervoor dat de configuratie van deze headers specifiek is afgestemd op de applicatie en de services die deze aanbiedt. Meer informatie kan hier worden gevonden: <a href="https://owasp.org/www-project-secure-headers/">https://owasp.org/www-project-secure-headers/</a></p>


Locatie van de kwetsbaarheid

dakkindercentra.nl

Score: 0



## ID: F.6 – Default Admin account actief binnen Azure

<b>RISICOCLASSIFICATIE</b> <b>Informatief</b>
<b>CVSS score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N</b>
<b>Owasp category: A04:2021 – Insecure Design</b>
<p><b>Beschrijving van de kwetsbaarheid of het risico</b></p> <p>Tijdens de analyse is gebleken dat het standaard beheerdersaccount binnen de Azure-omgeving nog steeds actief is. Hoewel dit op het eerste gezicht handig lijkt voor beheerdoeleinden, brengt het aanzienlijke beveiligingsrisico's met zich mee. Standaard admin-accounts zijn vaak een aantrekkelijk doelwit voor aanvallers, omdat deze accounts meestal voorspelbare namen hebben en hogere rechten binnen de omgeving bezitten. Dit vergroot de kans op brute-force aanvallen, credential stuffing en andere vormen van ongeautoriseerde toegang.</p> <p>Daarnaast kan het gebruik van een standaard admin-account leiden tot een gebrek aan traceerbaarheid. Wanneer meerdere beheerders hetzelfde account gebruiken, wordt het moeilijk om wijzigingen of verdachte activiteiten terug te leiden naar een specifieke gebruiker. Dit kan incident response bemoeilijken en risico's vergroten in het geval van een beveiligingsincident.</p> 
<p><b>Oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen</b></p> <p>Vitaen adviseert om het standaard admin-account uit te schakelen en over te stappen op individueel beheerde accounts met least privilege-principes. MFA (Multi-Factor Authenticatie) moet worden ingeschakeld voor alle beheerdersaccounts om de beveiliging verder te versterken. Daarnaast is het belangrijk om logging en monitoring in te richten, zodat verdachte inlogpogingen of ongebruikelijke activiteiten direct gedetecteerd kunnen worden.</p>




**Locatie van de kwetsbaarheid:**

Azure Omgeving

**Score: 0.0**



## ID: F.7 – Applicatiegeheim met te lange einddatum

RISICOCLASSIFICATIE	
Warning	
CVSS score: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N	
Owasp category: A05:2021 – Security Misconfiguration	
<p><b>Beschrijving van de kwetsbaarheid of het risico</b></p> <p>Tijdens de controle is vastgesteld dat een applicatiegeheim in Azure een ongebruikelijk lange einddatum heeft. Hoewel het instellen van een lange geldigheidstermijn misschien praktisch lijkt om frequente vernieuwing te vermijden, brengt dit aanzienlijke risico's met zich mee. Een geheim dat te lang geldig is, vergroot het aanvalsoppervlak: als het geheim ooit gelekt of gecompromitteerd raakt, blijft het bruikbaar voor een langere periode zonder dat iemand het doorheeft.</p> <p>Daarnaast kan een langlopende sleutel leiden tot beveiligingsverwaarlozing. Beheerders kunnen vergeten dat het geheim actief is, waardoor het jarenlang onopgemerkt en mogelijk zonder de juiste controle in gebruik blijft. Dit maakt het een aantrekkelijk doelwit voor aanvallers, vooral als het geheim brede toegangsrechten heeft binnen de Azure-omgeving.</p> <p>Zoals te zien in het screenshot, is het certificaat geldig tot 30-07-2035.</p>  <p><b>Oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen</b></p> <p>Vitaen adviseert om applicatiegeheimen een beperkte levensduur te geven, bij voorkeur niet langer dan 90 dagen. Dit dwingt regelmatige rotatie af en zorgt ervoor dat oude sleutels snel worden vervangen. Automatisering via Azure Key Vault en managed identities kan helpen om het beheer van geheimen</p>	

veiliger en efficiënter te maken. Verder is het essentieel om monitoring en logging in te richten, zodat het gebruik van applicatiegeheimen wordt gecontroleerd en misbruik vroegtijdig wordt opgemerkt.

**Locatie van de kwetsbaarheid:**

DAK Azure Tenant / Zorgmail Domainbook Update Script

**Score: 0.0**



## ID: F.9 – Verouderde Servers

<b>RISICOCLASSIFICATIE</b> <b>Warning</b>
<b>CVSS score: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N</b>
<b>Owasp category: A06:2021 – Outdated &amp; Vulnerable components</b>
<p><b><u>Beschrijving van de kwetsbaarheid of het risico</u></b></p> <p>Tijdens de controle is gebleken dat er nog steeds servers draaien op Windows Server 2008. Dit besturingssysteem heeft sinds januari 2020 geen ondersteuning of beveiligingsupdates meer van Microsoft. Dit betekent dat bekende kwetsbaarheden in het systeem niet worden gepatcht, waardoor aanvallers deze ongehinderd kunnen misbruiken.</p> <p>Verouderde systemen vormen een aantrekkelijk doelwit voor cybercriminelen, omdat exploits en aanvalsmethoden ruim beschikbaar zijn. Een ongepatchte server kan leiden tot ongeautoriseerde toegang, data-exfiltratie of zelfs volledige overname van de infrastructuur. Daarnaast kunnen compliance-regels, zoals ISO 27001 of NIS2, eisen stellen aan het up-to-date houden van IT-omgevingen, wat betekent dat het gebruik van verouderde software kan leiden tot non-compliance en mogelijke sancties.</p> <p>Het gaat hier om de volgende servers:</p> <ul style="list-style-type: none"><li>• fs01 - Windows Server 2008 R2 Enterprise Service Pack 1</li><li>• vc01 - Windows Server 2008 R2 Enterprise Service Pack 1</li><li>• app02 - Windows Server 2008 R2 Enterprise Service Pack 1</li></ul>
<p><b><u>Oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen</u></b></p> <p>Vitaen adviseert om Intune Compliance Policies strikter te configureren en ervoor te zorgen dat alleen conforme apparaten toegang krijgen tot bedrijfsbronnen. Dit kan worden bereikt door:</p> <ul style="list-style-type: none"><li>• Het afdwingen van minimale OS-versies en beveiligingsupdates.</li><li>• Het inschakelen van BitLocker-encryptie en Windows Defender.</li><li>• Het blokkeren van toegang voor niet-conforme apparaten via Conditional Access Policies.</li><li>• Regelmatige controles en rapportages op niet-conforme apparaten uit te voeren en gebruikers tijdig te informeren over compliance-vereisten.</li></ul>
<p><b>Locatie van de kwetsbaarheid:</b></p> <p>fs01 - Windows Server 2008 R2 Enterprise Service Pack 1</p>

vc01 - Windows Server 2008 R2 Enterprise Service Pack 1  
app02 - Windows Server 2008 R2 Enterprise Service Pack 1

**Score: 0.0**

