PINE DIGITAL SECURITY
Loire 130
2491 AJ Den Haag
Nederland

TELEFOON +31(0)70 – 311 10 10
E-MAIL info@pine.nl

www.pine.nl

KVK 55116183
BTW NR NL8515.71.943.B,01
IBAN NL41ABNA0422109290
BIC/SWIFT ABNANL2A

Third Party Mededeling

Voor	Kinderopvang Konnect B.V.
Product	Konnect
Versie	1.0
Door	Yannick Verhoeven
Datum	5 november 2015

1. Inleiding

Op verzoek van Kinderopvang Konnect B.V. verstrekt Pine Digital Security hierbij een Third Party Mededeling (TPM). Onderwerp van de TPM vormt de security test die Pine op verzoek van Kinderopvang Konnect B.V. in november 2015 heeft uitgevoerd op de Konnect applicatie.

2. Aanpak en scope

Pine Digital Security heeft een security test uitgevoerd aan de hand van versie 3.2 van de volgende checklists van Certified Secure[1]:

- Basic Web Application Scan Checklist
- Advanced Web Application Scan Checklist
- Basic Server Scan Checklist
- Advanced Server Scan Checklist

Tijdens een dergelijke security test wordt de applicatie door een ethical hacker handmatig getest met ondersteuning van tools. De tester zorgt dat aan het einde van de test, ieder item op bovengenoemde checklists gecontroleerd is. Hierdoor ontstaat een transparante en reproduceerbare test.

De rapportage bevat het resultaat van iedere check. Wanneer een checklist-item gefaald is, wordt uitgelegd op welke wijze de kwetsbaarheid zich voordoet, wat de impact is, en hoe deze kwetsbaarheid opgelost kan worden. Aan iedere kwetsbaarheid wordt bovendien een impact-score meegegeven die bepaald is volgens het CVSS(v2) model. Deze score duidt de technische impact van de kwetsbaarheid op de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens in het systeem.

Onderwerp van deze test was de Konnect webapplicatie. Deze is getest op de volgende URL's:

- https://test-security1.ouderportaal.nl
- https://test-security2.ouderportaal.nl
- https://demo.ouderportaal.nl/webservices/
- https://demo-admin.ouderportaal.nl

Naast de applicatie is ook de infrastructuur waarop de applicatie zich bevindt, getest. De scope van deze server scan was:

- 5.178.65.68: ouderportaal.wosah.nl (webserver)

Op de administratie omgeving heeft een test plaatsgevonden waarbij kwetsbaarheden die een ongeauthententiseerde aanvaller kan uitvoeren, door bijvoorbeeld een beheerder aan te vallen, zijn onderzocht.

Voor deze test zijn diverse gebruiker accounts gebruikt. De applicatie is getest vanuit de volgende gebruikersrollen:

- Beheerder
- Medewerker
- Ouder

[1] https://www.certifiedsecure.com/checklists/

3. Samenvatting resultaten

Tijdens de test is één kwetsbaarheid aangetroffen, met de volgende CVSS (v2) score:

CVSS (v2) score
2.6

De aangetroffen kwetsbaarheid betreft een zogeheten "defense in depth"-maatregel: deze kwetsbaarheid kan zelfstandig niet misbruikt worden, maar kan door een aanvaller worden gecombineerd met andere kwetsbaarheden om gegevens te stelen.

Binnen de applicatie zijn echter voldoende maatregelen getroffen waardoor het niet mogelijk is om andere kwetsbaarheden te gebruiken die benodigd zijn om de aangetroffen kwetsbaarheid te uit te buiten. Het is voor een aanvaller uiterst complex om deze kwetsbaarheid alsnog te misbruiken.

Pine Digital Security is gezien bovengenoemde kwetsbaarheden van mening dat de beveiliging van Konnect goed is.

Datum: 5 november 2015

Naam: C. Ottow

Functie: CTO

Handtekening: .....