Responsible disclosure

centrum veilig wonen

Bij Centrum Veilig Wonen vinden wij de veiligheid van onze systemen – ons netwerk, onze diensten en producten – erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is. Indien u een zwakke plek in één van onze systemen heeft gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen.

Zwakke plekken kunnen op twee manieren worden ontdekt: door ergens per ongeluk tegenaan te lopen bij normaal gebruik van een digitale omgeving, of door expliciet te proberen om een zwakheid te vinden.

Ons beleid voor responsible disclosure is geen uitnodiging om ons bedrijfsnetwerk uitgebreid actief te scannen om zwakke plekken te ontdekken. Wij monitoren ons bedrijfsnetwerk zelf. Hierdoor is de kans groot dat een scan wordt opgepikt, dat er door onze IT-afdeling onderzoek wordt gedaan en er mogelijk onnodige kosten worden gemaakt.

Voor onze producten bent u van harte uitgenodigd om in een offline en non-productie omgeving actief op zoek te gaan naar kwetsbaarheden en uw bevindingen aan ons te melden. Uit verantwoording tegenover de bewoners van Groningen en de partijen waar we werk aan uitbesteden, willen we niet oproepen tot hackpogingen op onze of hun infrastructuur. Echter, ook hiervoor geldt dat we zo snel mogelijk van u vernemen zodra er toch kwetsbaarheden worden gevonden in onze producten, zodat wij deze adequaat kunnen verhelpen.

Wij willen graag met u samenwerken onze systemen veiliger te maken.

Wij vragen u:

- Uw bevindingen zo snel mogelijk te mailen naar security@cvw.nl. Versleutel uw bevindingen met onze PGP key (0D47EFF5) om te voorkomen dat de informatie in verkeerde handen valt.
- De zwakheid niet te misbruiken door bijvoorbeeld het downloaden, veranderen of verwijderen van gegevens. Wij nemen uw melding altijd serieus en gaan elk vermoeden van een kwetsbaarheid uitzoeken, ook zonder ‘bewijs’.
- Het probleem niet met anderen te delen totdat het is opgelost.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, van social engineering of hacking tools, zoals vulnerability scanners.
- Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wat wij beloven:

- Wij reageren binnen 3 werkdagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet zonder uw toestemming met derden delen. Een uitzondering hierop is de politie en justitie, in geval van aangifte of indien gegevens worden opgeëist.
- Wij houden u op de hoogte van de voortgang van het oplossen van het probleem.
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker.

Met dank aan Floor Terra voor de voorbeeldtekst op http://responsibledisclosure.nl/

centrum veilig wonen

- Het is helaas niet mogelijk bij voorbaat juridische stappen tegen u uit te sluiten. We willen elke situatie apart kunnen wegen. We achten onszelf moreel verplicht om aangifte te doen op moment dat we het vermoeden hebben dat de zwakheid of gegevens misbruikt worden, of dat u kennis over de zwakheid met anderen heeft gedeeld. U kunt er op rekenen dat een toevallige ontdekking in onze online omgeving niet tot aangifte zal leiden.
- Als dank voor uw hulp bieden wij een beloning aan voor elke melding van een ons nog onbekend beveiligingsprobleem. De grootte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit van de melding.

Wij streven ernaar om alle problemen zo snel mogelijk op te lossen, alle betrokken partijen op de hoogte te houden en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

Met dank aan Floor Terra voor de voorbeeldtekst op http://responsibledisclosure.nl/