REGIONALE
BELASTING
GROEP

Responsible disclosure

De ICT-systemen van de Regionale Belasting Groep moeten natuurlijk veilig zijn. Daarom besteden we veel aandacht aan ICT-beveiliging. Toch kan het zijn dat u een zwakke plek in een van onze systemen ontdekt. We stellen het enorm op prijs als u die zwakke plek aan ons meldt, zodat we kunnen samenwerken om het probleem te onderzoeken en op te lossen. Wel is het van groot belang dat u dat op een verantwoorde manier doet. Voor ons, maar ook voor uzelf. U mag ervan uitgaan dat uw melding geen juridische gevolgen voor u heeft als u de onderstaande richtlijnen volgt.

Wij vragen u:

- Uw bevindingen te mailen naar info@derbg.nl.
- Uw melding zo snel mogelijk te doen nadat u de kwetsbaarheid hebt ontdekt.
- Het probleem niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of gegevens van derden in te kijken, verwijderen of aanpassen,
- Het probleem niet met anderen te delen totdat het is opgelost en alle vertrouwelijke gegevens die zijn verkregen via het lek direct na het dichten van het lek te wissen,
- 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.
- Uw contactgegevens achter te laten zodat we met u kunnen samenwerken aan een veilig resultaat. We hebben minimaal een e-mailadres of telefoonnummer van u nodig.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden, en

De volgende handelingen zijn niet toegestaan:

- Het plaatsen van malware, noch op onze systemen noch op die van anderen.
- Het zogeheten “bruteforcen” van toegang tot systemen
- Het gebruik maken van social engineering.
- Het openbaar maken of aan derden verstrekken van informatie over het beveiligingsprobleem voordat het is opgelost.
- Het verrichten van handelingen die verder gaan dan wat strikt noodzakelijk is om het beveiligingsprobleem aan te tonen en te melden. In het bijzonder waar het gaat om het verwerken (waaronder het inzien of kopiëren) van vertrouwelijke gegevens waar u door de kwetsbaarheid toegang toe heeft gehad. In plaats van een complete database te kopiëren, kunt u normaliter volstaan met bijvoorbeeld een directory listing. Het wijzigen of verwijderen van gegevens in het systeem is nooit toegestaan.
- Het gebruik maken van technieken waarmee de beschikbaarheid en/of bruikbaarheid van het systeem of services wordt verminderd (DoS-aanvallen).
- Het op wat voor (andere) wijze dan ook misbruik maken van de kwetsbaarheid.

Wat wij beloven:

- Wij reageren binnen 3 dagen 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 tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk,
- In dat overleg wordt een termijn afgesproken waarna de melder de kwetsbaarheid openbaar mag maken, bij voorkeur 60 dagen na melding van het probleem als het gaat om software en zes maanden bij hardware.
- Wij houden u op de hoogte van de voortgang van het oplossen van het probleem.
- Als u zich aan onze voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen betreffende de melding,
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker, en

Wij streven er naar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.