Responsible Disclosure

Fiksi vindt de veiligheid van haar platform erg belangrijk. Wij beveiligen ons platform op verschillende manieren, zoals door encryptie van gebruikersgegevens, SMS-toegangsverificatie en gebruik van een SSL-certificaat voor veilige gegevensoverdracht. Desondanks kan het voor¬komen dat er zich een zwakke plek in ons systeem bevindt.

Mocht u op zo'n zwakke plek stuiten, dan vernemen wij dit graag. Alleen op die wijze kunnen wij snel en adequaat maatregelen treffen het probleem te verhelpen. Wij stellen de samenwerking met u om onze gebruikers en ons platform beter te kunnen beschermen zeer op prijs.

Wat te doen als u een zwakke plek ontdekt?

Als u een zwakke plek ontdekt, verzoeken wij u het volgende:

- Geef voldoende informatie om het probleem te reproduceren. Zo kunnen wij het probleem zo snel mogelijk oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende. Bij ingewikkeldere kwetsbaarheden kan meer informatie nodig zijn.
- Laat contactgegevens (naam, e-mailadres en telefoonnummer) achter zodat wij contact met u kunnen opnemen.
- Doe de melding zo snel mogelijk na ontdekking van de kwetsbaarheid.
- Deel de informatie over het beveiligingsprobleem niet met anderen totdat het is opgelost.
- Ga verantwoordelijk om met de kennis over het beveiligingsprobleem. Verricht geen handelingen die verder gaan dan wat nodig is om het beveiligingsprobleem aan te tonen.

Geen juridische consequenties

Voldoet u bij uw melding aan deze voorwaarden? Dan verbinden wij geen juridische consequenties aan de melding.

Maak geen misbruik van een zwakke plek in een ICT-systeem

Als u een kwetsbaarheid ontdekt, maak hier dan geen misbruik van. Bijvoorbeeld door:

- Malware te plaatsen;
- Gegevens in een systeem te kopiëren, wijzigen of verwijderen (een alternatief hiervoor is een directory listing maken van een systeem);
- Veranderingen aan te brengen in het systeem;
- Herhaaldelijk toegang te verkrijgen tot het systeem of de toegang te delen met anderen;
- Gebruik te maken van het zogeheten 'bruteforcen' van toegang tot systemen;
- Gebruik te maken van denial-of-service of social engineering.

Wat Fiksi doet bij Responsible Disclosure

Heeft u een melding gedaan van een zwakke plek in een ICT-systeem? Wij behandelen deze melding als volgt:

- U krijgt binnen 1 werkdag een ontvangstbevestiging van ons.
- Wij reageren binnen 5 werkdagen op uw melding. Deze reactie bevat een beoordeling van de melding en een verwachte datum voor een oplossing.
- Wij houden u als melder op de hoogte van de voortgang van het oplossen van het probleem.
- Wij lossen het beveiligingsprobleem zo snel mogelijk op, maar uiterlijk binnen 30 dagen.
- Wij bepalen samen met u of en hoe over het gemelde probleem wordt bericht. Berichtgeving vindt pas plaats nadat het probleem is opgelost.
- Wij geven u een beloning als dank en blijk van waarderering voor de hulp.
- Wij behandelen uw melding vertrouwelijk. Fiksi deelt persoonlijke gegevens niet met derden zonder toestemming van u. Behalve als dit wettelijk of door een rechterlijke uitspraak verplicht is. Wij kunnen, als u dat wilt, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid.