Een beveiligingsprobleem ontdekt in onze diensten?

Laat het ons weten! Veiligheid van onze klantgegevens en systemen is voor ons heel belangrijk. Daarom werken wij voortdurend aan het veilig houden van onze diensten. Soms gaat er toch iets mis. Het is fijn als u ons dit laat weten, zodat wij maatregelen kunnen treffen.
Zo werken we samen aan het verbeteren van de veiligheid van onze gegevens en systemen.

Op deze pagina wordt onze responsible disclosure-procedure omschreven, inclusief wat wel en niet gemeld kan worden, de spelregels, en ons beloningsprogramma. De belangrijkste informatie wordt ook gestructureerd genoemd in onze **security.txt**. Let op dat onbeschikbare of incorrect functionerende websites en diensten niet via deze procedure gemeld kunnen worden.

Een onderdeel van het beloningsprogramma is een mogelijke opname in onze Hall of Fame:

Responsible Disclosure - Hall of Fame >

Deze responsible disclosure-procedure dekt alle Nederlandse merken van Achmea en een aantal internationale dochterbedrijven. Dit betreffen:

Nederlandse merken:

- Achmea
- Avéro Achmea
- Centraal Beheer
- De Christelijke Zorgverzekeraar
- De Friesland Zorgverzekeraar
- Eurocross
- FBTO
- InShared
- Interpolis
- Woonfonds
- Zilveren Kruis

Internationale dochterbedrijven:

- Achmea Australia

- Eureko Sigorta
- Interamerican
- Union

Een aantal van onze initiatieven valt ook onder deze procedure. Deze initiatieven betreffen:

- **Actify**
- **AutoModus**

Wat kunt u melden?

U kunt kwetsbaarheden in onze diensten melden. Voorbeelden zijn:

- Cross-Site Scripting (XSS) kwetsbaarheden.
- SQL injectie kwetsbaarheden.
- Zwakheden in inrichting beveiligde verbinding.
- Zwakheden in (mobiele) applicaties.

Wat kunt u niet melden?

Deze responsible disclosure-procedure is niet bedoeld voor het melden van klachten. Ook is de procedure niet bedoeld voor:

- het melden dat websites of diensten niet beschikbaar zijn.
- het melden van niet of incorrect werkende functies van websites of diensten.
- het melden van fraude.
- het melden van nep (phishing) e-mails.

Hoe kunt u melden?

Een ontdekte kwetsbaarheid in onze diensten kunt u melden via het contactformulier onderaan deze pagina of via het e-mailadres genoemd in onze **security.txt**.

Onderbouw in uw melding duidelijk hoe het beveiligingsprobleem kan worden misbruikt. Licht dit bij voorkeur toe met (bijvoorbeeld) schermafbeeldingen en een stap-voor-stap uitleg. Noem de exacte datum en tijd dat u het kwetsbaarheid gebruikte. Dit helpt ons met onze analyse van uw melding.

Spelregels

Wij vragen dat u uw bevinding alleen met de experts van Achmea deelt en het niet openbaar maakt. Het is fijn dat u ons de tijd geeft om de mogelijke kwetsbaarheid te analyseren en daarop gebaseerd acties uit te zetten.

Bij uw onderzoek van de gevonden kwetsbaarheid mag u geen systemen of diensten beschadigen. Verder mag de dienstverlening nooit opzettelijk onderbroken worden door uw onderzoek.

Mogelijk doet u bij uw onderzoek iets wat volgens wet- en regelgeving niet mag. Wij doen geen aangifte als u te goeder trouw en zorgvuldig handelt op de manier dat wij van u vragen.

Wij vragen u:

- alleen over de melding contact op te nemen met Achmea, via de kanalen behorend bij deze responsible disclosure-procedure.
- één bevinding per melding in te dienen.
- alleen te doen wat strikt noodzakelijk is om de kwetsbaarheid aan te tonen.
- geen social engineering toe te passen.
- geen algemene vulnerability scanning toe te passen.
- geen backdoor in een informatiesysteem te plaatsen, ongeacht het doel daarvan (zoals om een kwetsbaarheid aan te tonen).
- geen gegevens te kopiëren, te wijzigen of te verwijderen van of in onze systemen. Stuur ons alleen de (minimale) gegevens die u nodig heeft om het probleem aan te tonen. Maak bijvoorbeeld een directory listing van bestanden of schermafbeeldingen met enkel de informatie die nodig is om de kwetsbaarheid aan te tonen.
- de beschikbaarheid van onze systemen niet te beïnvloeden.
- geen zogenaamde ‘bruteforce attacks’ te gebruiken om in onze systemen te komen.
- de bevinding niet te delen met anderen.
- na de melding geen verdere pogingen uit te voeren om de kwetsbaarheid opnieuw te gebruiken.
- te reageren indien wij extra informatie over de ingediende melding vragen.

Wat doen wij met uw melding?

- Na ontvangst van uw melding, krijgt u van ons een automatische ontvangstbevestiging. Wij doen ons best om binnen drie werkdagen contact met u op te nemen over uw melding.
- Wij gebruiken uw contactgegevens alleen om met u over de melding te communiceren, en eventueel voor deelname aan het beloningsprogramma. Wij

delen uw gegevens niet met anderen, behalve als wij dit wettelijk verplicht zijn of als wij vermoeden dat u niet te goeder trouw handelt en zich schuldig maakt aan een strafbaar feit. In het laatste geval doen wij aangifte bij de politie.

- Als u anoniem meldt ontvangt u geen automatische ontvangstbevestiging en nemen wij geen contact met u op.

Voorwaarden van het beloningsprogramma

- Het bepalen of een beloning van toepassing is en welke beloning aangeboden wordt, doen wij op basis van het risico van het beveiligingsprobleem. Om in aanmerking te komen moet een melding terecht en nog niet eerder gemeld zijn, en de gemelde kwetsbaarheid moet significant zijn qua risico. Een beloning kan bestaan uit:

    - Een benoeming in de **Hall of Fame**, die bovenaan deze pagina en in onze **security.txt** genoemd wordt. Uiteraard doen wij dit enkel in overleg met en na goedkeuring van de melder. Wij behouden ons het recht om de informatie in de Hall of Fame te beperken.
    - Een T-shirt.
    - Cadeaubonnen tot een maximumbedrag van 300 euro.

- Een Beloning wordt niet aangeboden wanneer een melder of de melding zich niet aan de spelregels van deze procedure houden.
- Indien de melding geen beveiligingsprobleem betreft of een laag risico vormt, kan het zijn dat er geen beloning wordt aangeboden. Zie een niet-uitputtende lijst van kwetsbaarheden waarvoor geen beloning wordt uitgekeerd verderop op deze pagina.
- Wanneer dubbele meldingen worden ontvangen over een specifiek beveiligingsprobleem, wordt de beloning toegekend aan de eerste persoon die dit beveiligingsprobleem meldt. Achmea stelt vast of er sprake is van een dubbele melding en deelt geen inhoudelijke gegevens over de desbetreffende meldingen.
- Een toegekende beloning wordt slechts aan één persoon verstrekt.
- We proberen gelijke beloningen toe te kennen voor vergelijkbare beveiligingsproblemen. De beloningen en de in aanmerking komende beveiligingsproblemen kunnen echter wijzigen. Toegekende beloningen uit het verleden (bij Achmea of bij andere organisaties) bieden geen garantie voor aangeboden beloningen in de toekomst.

- Anonieme meldingen zijn uitgesloten van deelname aan het beloningsprogramma.

Uitzonderingen van het beloningsprogramma

Achmea kan, indien het gaat om een kwetsbaarheid met een laag of geaccepteerd risico, besluiten een melding niet te belonen. Hieronder staan enkele voorbeelden van dergelijke kwetsbaarheden. Deze lijst is niet uitputtend.

- HTTP 404-codes of andere niet HTTP 200-codes
- Toevoegen van platte tekst in 404-pagina's
- Versiebanners op publieke services
- Publiek toegankelijke bestanden en mappen met niet-gevoelige informatie
- Clickjacking op pagina's zonder inlogfunctie
- Cross-site request forgery (CSRF) op formulieren die anoniem toegankelijk zijn
- Ontbreken van 'secure' / 'HTTP Only' vlaggen op niet-gevoelige cookies
- Gebruik van de HTTP OPTIONS Method
- Host Header Injection
- Ontbreken van SPF, DKIM en DMARC records
- Ontbreken van DNSSEC
- Ontbrekende of incorrect toegepaste HTTP Security Headers, zoals:
    - Strict-Transport-Security (HSTS)
    - HTTP Public Key Pinning (HPKP)
    - Content-Security-Policy (CSP)
    - X-Content-Type-Options
    - X-Frame-Options
    - X-WebKit-CSP
    - X-XSS-Protection

Ook kunt u een melding maken, u kunt dat doen via het formulier op Achmea | Responsible Disclosure | Achmea