Beleid voor responsible disclosure (coordinated vulnerability disclosure)

Inleiding

Dit beleid geeft de uitgangspunten voor het verantwoord rapporteren van kwetsbaarheden in IT-systemen van Werkse!. Interne gebruikers en externe gebruikers, zoals websitebezoekers, worden opgeroepen om geconstateerde kwetsbaarheden te melden bij Werkse!.

Doel van het beleid

Bij Werkse! krijgt de beveiliging van onze IT-systemen hoge prioriteit. Ondanks de tijd en moeite die we hierin stoppen, kunnen er altijd kwetsbaarheden aanwezig zijn in de systemen.
Als je een dergelijke kwetsbaarheid ontdekt, vragen we je daarom ons hiervan op de hoogte te stellen. Op die manier kunnen wij actie ondernemen om de kwetsbaarheid zo snel mogelijk te verhelpen. Met jouw hulp kunnen wij onze systemen en (persoons)gegevens beter beschermen.

Uitgangspunten en vereisten

Wat wij van jou vragen:

- E-mail je bevindingen naar beveiligingsincidenten@werkse.nl. Zorg ervoor dat je e-mailverbinding veilig is, zodat de informatie niet in verkeerde handen valt.
- Maak geen gebruik van de kwetsbaarheid of het probleem dat je hebt ontdekt, bijvoorbeeld door meer gegevens te downloaden dan nodig om de kwetsbaarheid aan te tonen, of door gegevens in onze systemen te verwijderen of aan te passen.
- Maak de kwetsbaarheid niet bekend aan anderen, voordat de kwetsbaarheid verholpen is.
- Voer geen aanvallen uit op de fysieke of virtuele beveiliging, met behulp van social engineering, met gedistribueerde denial of service, met spam of schadelijke applicaties van derden.
- Geef voldoende informatie, zodat wij de kwetsbaarheid en de mogelijkheid van misbruik kunnen reproduceren. Op die manier kunnen wij het issue zo snel mogelijk oplossen.
  Meestal zijn het IP-adres of de URL van het getroffen systeem en een beschrijving van de kwetsbaarheid voldoende, maar bij complexe kwetsbaarheden is wellicht meer uitleg nodig.

Wat wij beloven:

- We zullen binnen drie (3) werkdagen op je melding reageren, met onze evaluatie van de melding en een verwachte datum voor een oplossing.

- Als je de bovenstaande instructies hebt opgevolgd, zullen we geen juridische stappen tegen je ondernemen met betrekking tot de melding.

- Wij behandelen je melding strikt vertrouwelijk en geven je persoonlijke gegevens niet zonder jouw toestemming door aan derden.

- We houden je op de hoogte van de voortgang bij het oplossen van het probleem.

- Als de kwetsbaarheid en oplossing openbaargemaakt worden, vermelden we je naam als de ontdekker van het probleem, tenzij je dit niet wenst.

- Als blijk van dank voor je hulp bieden wij een beloning aan voor elke melding van een beveiligingsprobleem waarvan wij nog niet op de hoogte waren. De hoogte van de beloning wordt bepaald op basis van de ernst van de kwetsbaarheid en de kwaliteit van de melding.

Wij streven naar snelle en passende opvolging van kwetsbaarheden. Ook spelen we graag een actieve rol in de publicatie van kwetsbaarheden en de (mogelijke) oplossing daarvan.

Reikwijdte

Systemen en services niet in scope

- Kwetsbaarheden in applicaties die Werkse! gebruikt, maar niet zelf beheert, zoals SaaS-applicaties.

- Kwetsbaarheden in een dienst die gekoppeld is aan onze websites, zoals een 'tag manager'.

Werkse! heeft geen operationele controle over dergelijke toepassingen. Het oplossen van kwetsbaarheden is in deze gevallen dan ook de verantwoordelijkheid van de betreffende leveranciers. Ondanks dat stellen we het op prijs als je ons op de hoogte stelt van een kwetsbaarheid bij onze softwareleveranciers. Onze opvolging valt dan alleen niet binnen dit beleid voor responsible disclosure.

Issues niet in scope

We bieden geen beloningen voor triviale issues die wij zelf ook monitoren, of voor kwetsbaarheden die niet daadwerkelijk benut kunnen worden door kwaadwillenden.
Voorbeelden van dergelijke issues:

- Basale HTTP security headers (bijvoorbeeld X-Frame-Options of Content-Security-Policy)

- SPF-, DKIM- en DMARC-configuratiekeuzes

- Clickjacking-gerelateerde issues.