Responsible Disclosure (Ned)

Bij de FDMediagroep vinden wij de veiligheid van onze systemen belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is.

Als u een zwakke plek in één van onze systemen heeft gevonden horen wij dit graag zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze klanten en onze systemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen te mailen naar security@fdmediagroep.nl;
- 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;
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden; en
- 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.
- Het CVE nummer van de kwetsbaarheid in de mail te vermelden.

Wat wij beloven:

- Wij reageren binnen 5 dagen met een reactie op het rapport;
- Als u zich aan bovenstaande voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen betreffende de melding;
- 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;
- 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; en
- 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 met een minimum van €50,- .

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.

FDMG kan beslissen dat een mogelijke kwetsbaarheid met een laag of geaccepteerd risico niet beloond wordt. Enkele voorbeelden van kwetsbaarheden die buiten de scope van het programma vallen:

- 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