Novelist

1. Inleiding

Novelist, een handelsnaam van Amdax B.V., verwelkomt feedback van beveiligingsonderzoekers en het publiek om de veiligheid van haar systemen te verbeteren. Indien je denkt een kwetsbaarheid, privacy probleem, blootgestelde gegevens of een ander beveiligingsprobleem te hebben ontdekt in een van onze digitale omgevingen, stellen wij het op prijs dat je dit bij ons meldt. Dit beleid beschrijft de stappen voor het melden van kwetsbaarheden, wat wij van melders verwachten en wat jij van ons mag verwachten in ruil daarvoor.

2. Reikwijdte

Dit beleid is van toepassing op alle digitale activa die eigendom zijn van, worden beheerd door of worden onderhouden door Amdax B.V. Elke ontwerpfout of implementatieprobleem dat de vertrouwelijkheid of integriteit van gebruikersgegevens wezenlijk beïnvloedt, valt in beginsel binnen de reikwijdte van dit programma. Hoewel dit beleid gericht is op beveiligingsonderzoek, staan wij open voor meldingen over alle producten en diensten die onder direct beheer van Amdax B.V. vallen, waaronder ook open-sourcecomponenten, software of onderdelen van derden.

De volgende onderwerpen vallen echter niet binnen de reikwijdte van dit programma en zullen niet resulteren in het publiceren van een kwetsbaarheid:

- *HTTP security headers, including but not limited to CSP, HSTS and X-XSS-Protection;*
- *Non-200 HTTP return codes;*
- *Version banners or other service fingerprinting;*
- *Clickjacking and/or tabnapping;*
- *Missing Secure/HTTPOnly flags on non-sensitive Cookies;*
- *E-mail domain and server settings, including DMARC, DKIM and SPF issues;*
- *Any SSL/TLS issue, including potential weak algorithm support, without a working PoC*.

Let op: dit beleid vormt **geen** uitnodiging om onze netwerken of systemen geautomatiseerd te scannen op kwetsbaarheden, hetgeen kan leiden tot overbelasting of excessief verkeer op onze systemen.

3. Onze verwachtingen

Wij verwachten van de beveiligingsonderzoekers en het publiek dat zij:

- Te allen tijde te goeder trouw handelen en privacy inbreuken, verstoring van onze dienstverlening, schade aan productieomgevingen of dataverlies vermijden tijdens hun onderzoek;
- Gevonden kwetsbaarheden zo spoedig mogelijk melden;
- Uitsluitend gebruik maken van de officiële kanalen om kwetsbaarheden bij ons te melden – dit kan via e-mail aan: rd@amdax.com, voorzien van alle relevante informatie. Hoe gedetailleerder de melding, hoe efficiënter wij kunnen beoordelen en oplossen. Gevoelige informatie dient te worden gedeeld via de volgende GPG sleutel;
- Alleen onderzoek uitvoeren binnen de hierboven beschreven scope;
- Alleen eigen accounts of testaccounts gebruiken tijdens het onderzoek, en geen toegang verkrijgen tot of wijzigingen aanbrengen in onze gegevens of die van onze gebruikers;
- Informatie over geconstateerde kwetsbaarheden vertrouwelijk houden totdat wij 90 dagen de gelegenheid hebben gehad om het probleem op te lossen;

- Indien een kwetsbaarheid onbedoelde toegang tot gegevens oplevert: beperk de hoeveelheid gegevens die je benadert tot het strikt noodzakelijke om een *proof of concept* effectief aan te tonen, staak het onderzoek onmiddellijk en dien direct een melding in zodra je tijdens het testen gebruikersgegevens aantreft, zoals persoonsgegevens (PII) of andere vertrouwelijke of bedrijfseigen informatie.

4. Wat van ons verwacht kan worden

Indien je in overeenstemming met dit beleid met ons samenwerkt, mag je van Novelist het volgende verwachten:

- Binnen drie werkdagen reageren op je melding en met je samen werken om deze te begrijpen en te valideren;
- Jou op de hoogte te houden van de voortgang van de behandeling van de kwetsbaarheid;
- Vastgestelde kwetsbaarheden binnen redelijke termijn op te lossen, rekening houdend met operationele beperkingen;
- Jouw bijdrage te erkennen indien je de eerste bent die een unieke kwetsbaarheid meldt die leidt tot een aanpassing in onze code of configuratie;
- Voor zover redelijk of wettelijk vereist, geen juridische stappen te ondernemen of te ondersteunen ten aanzien van je bevindingen en onderzoek;
- Als blijk van waardering een beloning toe te kennen voor elke melding van een tot dan toe onbekend beveiligingsprobleem. De hoogte van de beloning wordt bepaald op basis van de ernst van de kwetsbaarheid en de kwaliteit van de melding.