Responsible Disclosure policy

17/02/2023

AMARON B.V. (S.R.L.)
Kapellestraat 13
8755 Ruiselede
T +32 (0)51 62 73 20
F +32 (0)51 43 33 81

TVA BE 0812.300.071
IBAN BE96 0017 0057 5405
BIC GEBABEBB

1 Inhoudstafel

2 Het doel van deze policy

Amaron wil zo snel mogelijk oplossingen kunnen vinden voor gevonden kwetsbaarheden, rekening houden met de ernst van de kwetsbaarheid. Amaron toont appreciatie voor partijen die kwetsbaarheden rapporteren, indien zij ethisch en in lijn met het wettelijk kader voor ethisch hacken te werk gaan.

3 Hoe een security kwetsbaarheid rapporteren?

Contacteer onmiddellijk Amaron via privacy@amaron.be en dit niet later dan 72 uur nadat de kwetsbaarheid werd gevonden. Wij vragen u ons de volgende gegevens mee te delen, zodat Amaron in staat is een grondige analyse te doen en de kwetsbaarheid te reproduceren:

- Beschrijving van de kwetsbaarheid
    - Soort van kwetsbaarheid
    - Configuratiedetails
    - Besturingssystemen
    - IP-adres of URL van het betrokken systeem:
    - Stap voor stap, inclusief data en tijdstippen, hoe u tot de kwetsbaarheid bent gekomen
- Voeg printscreens toe zodat wij de kwetsbaarheid beter kunnen analyseren. Eventuele persoonsgegevens dienen onkenbaar te worden gemaakt op de printscreens.
- Uw naam, organisatienaam en contactgegevens, inclusief telefoonnummer om u terug te contacteren.

Al deze gegevens dienen te worden doorgestuurd in een document dat beveiligd is met een complex paswoord. Het paswoord dient u ons door te bellen door ons te contacteren op +32 51 62 73 20.

Wij houden deze gegevens bij op lange termijn in kader van een mogelijks geschil.

4 Hoe ga je om met een kwetsbaarheid?

Het is belangrijk te allen tijde de GDPR regels te respecteren. Indien de partij toegang krijgt tot gegevens door de kwetsbaarheid, is het ten striktste verboden deze te verwerken.

Het moet duidelijk zijn dat zaken als phishing, spamming, brute force aanvallen, DDoS, het kopiëren of verwijderen van gegevens, het installeren van malware of schade toebrengen aan het systeem of de gegevens expliciet verboden zijn.

5 Samenwerking

Het doel is voor beide partijen om tot een oplossing komen om negatieve gevolgen te voorkomen. De partij die de kwetsbaarheid ontdekt is daarom ook verplicht om kosteloos bijstand te verlenen aan Amaron. Amaron kan een beloning voorzien indien veel tijd wordt gevraagd van de partij die de kwetsbaarheid heeft ontdekt. In het geval van geautoriseerde activiteiten (bijvoorbeeld penetration testing in opdracht van Amaron) wordt dit wel vergoed volgens de overeenkomst met de partij.

6 Rapportage en publicatie van kwetsbaarheden

Enkel Amaron kan beslissen of de kwetsbaarheid wordt meegedeeld met zijn klanten, het Cyber Security Belgium, de gegevensbeschermingsauthoriteit, de politie of andere relevante partijen. De partij (bijvoorbeeld een ethisch hacker) die de kwetsbaarheid vond mag deze beslissing niet nemen. Het is strikt verboden om de kwetsbaarheid publiekelijk kenbaar te maken door de partij die de kwetsbaarheid vond. Opgelet, weet dat u strafbaar bent wanneer u:

- Hacking doet om schade toe te brengen of met bedrieglijke opzet.
- Hacking doet met goede intenties, maar u dit niet in lijn doet met de ethical hacking wet of GDPR wet.
- Als u zich niet houdt aan de regels van deze policy.

7 Geschillen

Deze policy wordt beheerst door het Belgisch recht. Geschillen worden voorgelegd aan de rechtbanken/hoven in het gerechtelijk arrondissement West-Vlaanderen, afdeling Brugge, die exclusieve territoriale bevoegdheid hebben.

8 Wijzigingen aan deze policy

Wij behouden ons het recht voor om de inhoud van deze Policy op elk gewenst moment te wijzigen, of om de Policy te beëindigen.