MageHost B.V. | Responsible disclosure

Januari 2021

We besteden veel zorg en aandacht aan de veiligheid en integriteit van onze systemen en diensten. Toch kan het uiteraard voorkomen dat er een zwakke plek, kwetsbaarheid, exploit of ander beveiligingsrisico wordt ontdekt (hierna: “beveiligingsrisico”).

We willen jou graag verzoeken om eventueel door jou gevonden beveiligingsrisico’s, met inachtneming van het onderstaande beleid, zo snel mogelijk bij ons te melden. Dit stelt ons in staat om de beveiliging van onze systemen en diensten te blijven verbeteren en continu te blijven streven naar een zo veilig mogelijke ervaring voor onze klanten en gebruikers.

Wij vragen je hiervoor:

1. tijdens jouw onderzoek:
    - geen gebruik te maken van distributed denial of service aanvallen (DDoS);
    - geen gebruik te maken van ‘brute force’ aanvallen;
    - geen malware te plaatsen;
    - geen gebruik te maken van phishing en/of hacking tools;
    - geen veranderingen aan te brengen in systemen of de daarin opgeslagen gegevens;
    - geen gebruik te maken van social engineering of aanvallen op de fysieke beveiligingsmaatregelen;
    - geen gebruik te maken van spam;
2. tijdens jouw onderzoek niet verder te gaan dan wat strikt noodzakelijk is om de beveiligingsrisico’s conform dit beleid met ons te delen en deze niet te misbruiken door bijvoorbeeld gegevens van derden te benaderen, systemen te overbelasten of op andere manieren overlast te creëren voor gebruikers van de systemen;
3. de beveiligingsrisico’s en al je daaraan gerelateerde bevindingen te melden via info@magehost.pro, met voor zover mogelijk:
    - een zo duidelijk mogelijke omschrijving van het beveiligingsrisico;
    - het IP-adres of de URL van het betreffende systeem; en
    - duidelijk beschreven stappen waarmee wij de bevinding kunnen reproduceren en/of vaststellen;
4. jouw bevindingen strikt geheim te houden en niet met anderen te delen totdat het betreffende beveiligingsrisico is verholpen; en
5. alle eventueel vertrouwelijke gegevens die als gevolg van het onderzoek in jouw bezit zijn gekomen te wissen zodra het betreffende beveiligingsrisico is verholpen.

Van ons kan je verwachten dat:

1. als je bij het onderzoeken en melden van je bevindingen de in dit beleid beschreven procedure volgt, wij geen juridische consequenties zullen verbinden aan je melding.
2. alle meldingen vertrouwelijk worden behandeld en dat jouw persoonlijke gegevens niet zonder toestemming met derden zullen worden gedeeld, tenzij dit op grond van de wet of een rechterlijke uitspraak verplicht is.
3. wij jou, als je dat wil en indien er sprake is van (publieke) communicatie of publicatie over het beveiligingsrisico, vermelden als ontdekker van het beveiligingsrisico (N.B. het kan voorkomen dat een ander het betreffende beveiligingsrisico eerder heeft ontdekt, maar dat dit nog niet bekend is gemaakt. In dat geval wordt die ander beschouwd als de ontdekker.);

4. wij binnen 7 dagen reageren op jouw melding met onze beoordeling van je bevindingen en een verwachte datum van oplossing.
5. wij hard zullen werken om tot een oplossing te komen voor het beveiligingsrisico en jou op de hoogte zullen houden over de voortgang van de oplossing; en
6. wij, nadat het beveiligingsrisico is verholpen, in beginsel open staan voor het leveren van bijdragen aan eventuele publicaties van jouw bevindingen.

Wij bieden geen beloningen voor het melden van beveiligingsrisico's.