Responsible disclosure

Kwetsbaarheid ontdekt? Laat het ons weten.

Bij Pon Holdings B.V. en haar dochterondernemingen vinden we de veiligheid van onze systemen en ons netwerk erg belangrijk. We zijn ervan overtuigd dat een goede beveiliging essentieel is voor het vertrouwen dat onze klanten, leveranciers en medewerkers in ons stellen. Ondanks de zorg voor de beveiliging van onze systemen zou het kunnen voorkomen dat een kwetsbaarheid wordt ontdekt.

Middels ons *responsible disclosure* beleid vragen wij iedereen die een kwetsbaarheid ontdekt, dit zo snel mogelijk te melden zodat we adequate maatregelen kunnen treffen. We werken graag met u samen om de kwetsbaarheid op te lossen. Ons *responsible disclosure* beleid is geen uitnodiging om ons bedrijfsnetwerk uitgebreid actief te scannen om kwetsbaarheden te ontdekken. Wij monitoren ons netwerk zelf.

Wij vragen u:

- Uw bevindingen zo snel mogelijk te versturen naar rd@pon.com. Als u de melding versleuteld wilt versturen, meld dit dan in uw e-mail. Wij geven u dan instructies;
- Ons voldoende informatie te geven om de kwetsbaarheid 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 informatie nodig zijn;
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld het downloaden, inzien, verwijderen of aanpassen van gegevens;
- Kwetsbaarheden niet met anderen te delen totdat de kwetsbaarheid is opgelost. Mocht u onverhoopt vertrouwelijke gegevens hebben verkregen dan vragen wij u deze gegevens direct te wissen;
- Geen gebruik te maken van aanvallen op fysieke beveiliging of applicaties van derden, social engineering, distributed denial of service (DDoS), spam of hacking tools zoals vulnerability scanners.

Wat mag u verwachten:

- Wij nemen uw melding altijd serieus. Ook vermoedens van kwetsbaarheden zullen wij onderzoeken;
- Wij reageren binnen 5 werkdagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing;
- Wij houden u op de hoogte van de voortgang van het oplossen van de kwetsbaarheid;
- Als u zich aan bovenstaande voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen betreffende de melding. Het Openbaar Ministerie behoudt altijd het recht om zelf te beslissen of vervolgonderzoek nodig is;
- 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, zoals wanneer uw gegevens worden opgevraagd door politie en justitie;
- Een anonieme melding betekent mogelijk dat wij geen contact met u kunnen opnemen over bijvoorbeeld de vervolgstappen en voortgang van het dichten van de kwetsbaarheid;
- We kunnen onze blijk van waardering tonen met een maximale waarde van € 50. Dit wordt bepaald aan de hand van de ernst van de kwetsbaarheid en kwaliteit van de melding;
- In eventuele berichtgeving over de gemelde kwetsbaarheid zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker;
- Wij streven ernaar alle kwetsbaarheden zo snel mogelijk te analyseren en indien nodig op te lossen. We zullen daarbij alle betrokken partijen op de hoogte houden.

Dit *responsible disclosure* beleid is gebaseerd op de leidraad Responsible Disclosure van het Nationaal Cyber Security Centrum en het voorbeeld Responsible Disclosure geschreven door Floor Terra.