Coordinated Vulnerability Disclosure

Wij nemen de veiligheid van onze systemen en gebruikers zeer serieus en hechten veel waarde aan het verbeteren hiervan. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat een zwakke plek in de systemen te vinden is. Om kwaadwillenden een stap voor te blijven, willen we graag dat iedereen die een kwetsbaarheid in onze systemen vindt dat aan ons meldt. Door het maken van een melding verklaar je als melder akkoord te gaan met onderstaande afspraken over *Coordinated Vulnerability Disclosure* en zullen wij de melding conform onderstaande afspraken afhandelen.

Wij vragen het volgende van je:
- Je vermijdt schending van privacy, verslechtering van de gebruikerservaring, verstoring aan productiesystemen en vernietiging van gegevens tijdens beveiligingstests;
- Je houdt informatie over kwetsbaarheden die je ontdekt hebt vertrouwelijk tussen jezelf en ons en geeft ons mimimaal 90 dagen om het probleem op te lossen.

Wat mag u van ons verwachten:
- Wij werken met je samen om de kwetsbaarheid te begrijpen en snel op te lossen (waaronder een eerste bevestiging van uw melding binnen 72 uur na indiening daarvan);
- Wij houden je op de hoogte van onze pogingen om de kwetsbaarheid op te lossen;
- Wij nemen geen wettelijke maatregelen ten aanzien van jouw onthulling.

Wat is <u>niet</u> toegestaan:
Vanwege de veiligheid van onze gebruikers, medewerkers, het internet in het algemeen en jou als beveiligingsonderzoeker zijn de volgende handelingen niet toegestaan:
- het testen van applicaties die niet onder het beheer van Progresity vallen;
- social engineering en fysieke testen (bijvoorbeeld phishing, tailgating);
- het testen van network level denial of service (DoS/DDoS)-kwetsbaarheden.
- het plaatsen van malware.
- gegevens in het systeem kopiëren, wijzigen of verwijderen.
- veranderingen aanbrengen in het systeem.

Wat we niet van je wensen te ontvangen, zijn:
- persoonlijk identificeerbare informatie (PII); en
- betalingsgegevens, zoals bankrekeningnummers en creditcardgegevens.

Rietbaan 10, 2908 LP Capelle aan den IJssel
- T 088 770 4800
- info@progresity.com
- www.progresity.com

Progresity is onderdeel van Conxillium

Hoe meldt je een beveiligingskwetsbaarheid aan ons?
Als je denkt dat je in een van onze producten of platformen een beveiligingskwetsbaarheid hebt gevonden, meld deze dan per e-mail aan security@progesity.com. Versleutel de bevindingen indien mogelijk om te voorkomen dat de informatie in verkeerde handen valt.

Vergeet niet de volgende details aan de melding toe te voegen:
- een beschrijving van de locatie en de potentiële impact van de kwetsbaarheid;
- een gedetailleerde beschrijving van de stappen die nodig zijn om de kwetsbaarheid te reproduceren (POC-scripts, screenshots en gecomprimeerde schermafbeeldingen worden gewaardeerd).

N.B. voor het melden van een kwetsbaarheid m.b.t. producten of platformen van andere organisaties binnen de Conxillium Group verwijzen wij je door naar het Responsible Disclosure beleid op de website van de bijbehorende organisatie.