

Vulnerability Disclosure Policy (VDP)

Scope

Deze policy is van toepassing op:

- Alle webapplicaties en mobiele applicaties ontwikkeld door Breman.
- Servers, netwerken en andere infrastructuurelementen gebruikt door Breman.

Gedragscode

Wij vragen dat onderzoekers:

- Geen vertrouwelijke gegevens, inclusief persoonlijke gegevens van gebruikers, zonder toestemming bekijken, wijzigen of verwijderen.
- Testen uitvoeren op systemen die onder de scope van deze policy vallen.
- Geen DoS (Denial of Service) aanvallen uitvoeren.
- Geen 'social engineering' aanvallen uitvoeren.

Rapportageproces

Om een kwetsbaarheid te rapporteren, verzoeken wij onderzoekers om:

1. Een gedetailleerde beschrijving van de kwetsbaarheid te geven, inclusief de locatie en mogelijke impact.
2. Stappen te beschrijven die nodig zijn om de kwetsbaarheid te reproduceren.
3. Screenshots of video's bij te voegen die het probleem duidelijk illustreren.
4. Contactinformatie te verschaffen voor eventuele opvolgvraagstukken.

Verwachtingen van Breman

Bij ontvangst van een kwetsbaarheidsrapport zullen wij:

- Binnen 5 werkdagen de ontvangst van het rapport bevestigen.
- De onderzoeker op de hoogte houden van de voortgang van het probleem en de oplossing.
- De onderzoeker informeren wanneer de kwetsbaarheid is opgelost.
- Open en transparant communiceren gedurende het hele proces.

Beloningen en Erkenning

Afhankelijk van de ernst van de kwetsbaarheid en de kwaliteit van het rapport, kunnen wij:

- Cadeaubonnen en/of andere goodies.
- Erkenning, dankbaarheid en referenties.
- Taart of pizza.

Juridische Overwegingen

We zullen geen juridische stappen ondernemen tegen onderzoekers die zich aan deze policy houden. We behouden ons het recht voor om juridische stappen te ondernemen tegen degenen die de policy schenden of proberen onze systemen te compromitteren zonder enige verantwoordelijkheid of eerlijkheid.

Privacy en Verantwoordelijkheid

Alle persoonlijke gegevens die door onderzoekers worden verstrekt, worden alleen gebruikt voor communicatie over het gemelde beveiligingsprobleem. Wij behandelen alle rapporten vertrouwelijk en delen geen informatie met derden zonder toestemming van de onderzoeker, tenzij wettelijk verplicht.

Slotopmerkingen

Wij waarderen de inspanningen van de beveiligingsgemeenschap en streven ernaar om een veilige en betrouwbare digitale omgeving te creëren. Door samen te werken, kunnen we onze diensten en systemen voortdurend verbeteren en beschermen tegen potentiële bedreigingen.

Bedankt voor uw hulp en samenwerking in het verbeteren van onze veiligheid. Indien u vragen heeft over deze policy of het melden van kwetsbaarheden, neem dan contact met ons op via ictsupport@breman.nl.

