bunq
www.bunq.com
+31(0) 20 205 1337
Naritaweg 131-133
1043 BS Amsterdam
KvK 54992060
Versie: 2

Responsible Disclosure Beleid

bunq

Kwetsbaarheden melden

De veiligheid van jouw geld en data is onze topprioriteit. Daarom werken we hard om onze systemen te beschermen. Heb je toch een zwakke plek in onze systemen gevonden? Help ons door deze kwetsbaarheid direct door te geven.

We willen onze fouten niet verbergen, maar het openbaar maken van zwakke plekken kan grote gevolgen hebben voor al onze gebruikers. Maak een kwetsbaarheid daarom niet zomaar openbaar. Om te voorkomen dat gebruikers schade lijden, vragen we je om eerst samen met ons aan een oplossing te werken.

Hoe kan ik een melding doen?

Stuur een e-mail naar responsible-disclosure@bunq.com en versleutel deze indien mogelijk met onze GPG-sleutel (ID 40B8B050) om te voorkomen dat de informatie in verkeerde handen valt.

Leg in je e-mail kort uit welke kwetsbaarheid je hebt gevonden. Geef ons hierbij voldoende informatie om het probleem te kunnen reproduceren/onderzoeken.

Kan ik een zwakke plek ook anoniem melden?

Ja, je hoeft je naam en contactgegevens niet door te geven als je een melding doet.

De spelregels

Het kan voorkomen dat je bij het ontdekken van een kwetsbaarheid handelingen hebt verricht die strafbaar zijn. Wij doen geen aangifte en dienen geen schadeclaim in als je je aan de volgende spelregels houdt:

- ga verantwoordelijk om met de kennis over de kwetsbaarheid en verricht geen handelingen die verder gaan dan noodzakelijk voor het aantonen van de zwakke plek;
- zorg ervoor dat je tijdens het onderzoeken geen schade aanricht;
- maak geen gebruik van denial-of-service of social engineering;
- zorg ervoor dat je onderzoek niet leidt tot een onderbreking van onze dienstverlening;
- je onderzoek mag niet tot gevolg hebben dat bank- en/of klantgegevens openbaar worden;
- plaats geen backdoor. Ook niet om een kwetsbaarheid aan te tonen;
- wijzig of verwijder geen gegevens. Is het voor je onderzoek nodig om gegevens te kopiëren? Kopieer dan nooit meer gegevens dan nodig;
- breng geen systeemveranderingen aan;
- probeer niet vaker dan nodig een systeem binnen te dringen;
- gebruik geen bruteforce-technieken;
- gebruik geen technieken die de beschikbaarheid van onze diensten kunnen beïnvloeden.

Verder is het voor ons belangrijk dat je een melding zo snel mogelijk doet. Vraag ons ook eerst even om toestemming voordat je de kwetsbaarheid openbaar maakt.

bunq

Wat gebeurt er met mijn melding?

Als we jouw melding binnen hebben, gaan wij de kwetsbaarheid onderzoeken. We doen ons best om binnen een paar dagen op je melding te reageren en we houden je op de hoogte van de voortgang van onze werkzaamheden. Hoeveel tijd we voor het oplossen nodig hebben, is afhankelijk van de complexiteit van het probleem. We vragen je om ook na je melding het probleem niet direct openbaar te maken, maar om ons de tijd te geven het probleem op te lossen.

Wordt de kwetsbaarheid die ik gemeld heb openbaar gemaakt?

Samen kunnen we besluiten of en op welke manier de door jou gemelde kwetsbaarheid (nadat deze is opgelost) openbaar wordt gemaakt. Als je het wil, vermelden we jouw naam hierbij.

Krijg ik een beloning voor mijn melding?

Als dank voor je hulp kunnen we je een beloning aanbieden. Dit doen we alleen als je een voor ons nog onbekende kwetsbaarheid hebt gemeld. De beloning bepalen we aan de hand van je melding, hierbij houden wij onder andere rekening met de ernst van de gemelde kwetsbaarheid. Mochten meerdere mensen tegelijk dezelfde kwetsbaarheid bij ons melden, dan belonen wij alleen de eerste melder.

Hoe zit het met mijn privacy?

Je persoonsgegevens worden alleen gebruikt om actie te ondernemen naar aanleiding van je melding. We geven je gegevens niet zonder toestemming aan anderen, behalve als we op grond van de wet of een gerechtelijke uitspraak je gegevens moeten afstaan.

Als we een ander bedrijf inschakelen om je melding verder te onderzoeken, kan het nodig zijn dat wij je gegevens aan dit bedrijf doorgeven. We zorgen er dan altijd voor dat ook dit bedrijf je gegevens geheimhoudt.

Wet- en regelgeving

Hou altijd rekening met de toepasselijke wet- en regelgeving. Je zou namelijk alsnog met justitie in aanraking kunnen komen, ook als wij je niet aan justitie rapporteren.