Proxhost | Responsible disclosure

Laatst bijgewerkt: 15 mei 2026

1. Inleiding

We besteden veel zorg en aandacht aan de veiligheid en integriteit van onze systemen en diensten. Toch kan het voorkomen dat er een zwakke plek, kwetsbaarheid, exploit of ander beveiligingsrisico wordt ontdekt. In dit beleid noemen we dit een beveiligingsrisico.

We vragen je om beveiligingsrisico's zo snel mogelijk bij ons te melden volgens dit responsible disclosure beleid. Daarmee help je ons om de beveiliging van onze systemen en diensten te verbeteren en klanten en gebruikers beter te beschermen.

2. Scope van dit beleid

Dit beleid is van toepassing op systemen, websites, klantportalen, infrastructuur en diensten die door Proxhost worden beheerd.

Systemen van klanten of derde partijen vallen alleen binnen deze scope wanneer Proxhost daar expliciet beheer over voert of wanneer vooraf schriftelijk toestemming is gegeven. Test niet op klantomgevingen of systemen van derden zonder duidelijke toestemming.

3. Wat wij van jou vragen

Tijdens je onderzoek vragen wij je om zorgvuldig, proportioneel en te goeder trouw te handelen. Ga niet verder dan strikt noodzakelijk is om het beveiligingsrisico vast te stellen en met ons te delen.

- maak geen gebruik van distributed denial of service-aanvallen (DDoS) of andere methoden die systemen kunnen overbelasten;
- voer geen brute-force-aanvallen uit en probeer geen wachtwoorden of tokens te raden;
- plaats geen malware, backdoors, shells of andere persistente toegang;
- maak geen gebruik van phishing, credential harvesting, social engineering of aanvallen op fysieke beveiligingsmaatregelen;
- gebruik geen tooling of onderzoeksmethoden die schade veroorzaken, gegevens wijzigen, systemen verstoren of ongeautoriseerde toegang uitbreiden;
- breng geen wijzigingen aan in systemen, configuraties of opgeslagen gegevens;
- download, kopieer, wijzig of verwijder geen klantdata of persoonsgegevens, behalve wanneer dit strikt noodzakelijk is voor een minimale proof-of-concept;
- gebruik geen accounts van anderen en probeer geen rechten uit te breiden buiten wat nodig is voor de melding;
- veroorzaak geen verstoring op productieomgevingen en voorkom overlast voor klanten, gebruikers of andere systemen;
- houd je bevindingen strikt vertrouwelijk totdat het beveiligingsrisico is verholpen en publicatie is afgestemd met Proxhost;
- wis alle vertrouwelijke gegevens die je tijdens het onderzoek mogelijk hebt verkregen zodra het beveiligingsrisico is verholpen of zodra wij daarom vragen.

4. Hoe je een beveiligingsrisico meldt

Meld beveiligingsrisico's bij voorkeur via security@proxhost.nl. Als deze mailbox nog niet actief is, zorg er dan voor dat deze wordt aangemaakt of doorgestuurd voordat dit beleid wordt gepubliceerd.

Vermeld in je melding, voor zover mogelijk:

- een duidelijke omschrijving van het beveiligingsrisico;
- het IP-adres, domein, de URL of het systeem waarop de bevinding betrekking heeft;
- de stappen waarmee wij de bevinding kunnen reproduceren of vaststellen;
- de mogelijke impact van het beveiligingsrisico;
- eventuele screenshots, logging of beperkte proof-of-concept informatie, voor zover dit nodig is en geen onnodige gevoelige data bevat.

Deel geen gevoelige gegevens in je melding, tenzij dit strikt noodzakelijk is. Wanneer aanvullende gevoelige informatie nodig is, stemmen wij samen een veilige manier af om deze informatie te delen.

5. Wat je van ons mag verwachten

- Wij bevestigen de ontvangst van je melding zo snel mogelijk, bij voorkeur binnen twee werkdagen.
- Binnen zeven dagen geven wij, waar mogelijk, een eerste inhoudelijke reactie met onze beoordeling en de verwachte vervolgstappen.
- Wij behandelen je melding vertrouwelijk en delen je persoonsgegevens niet zonder toestemming met derden, tenzij dit wettelijk verplicht is of noodzakelijk is op grond van een rechterlijke uitspraak.
- Wij werken aan een passende oplossing voor het beveiligingsrisico en houden je, waar redelijk mogelijk, op de hoogte van de voortgang.
- Als je dat wilt en er sprake is van publieke communicatie of publicatie, kunnen wij je vermelden als ontdekker van het beveiligingsrisico, tenzij een ander het beveiligingsrisico eerder heeft gemeld of ontdekt.
- Nadat het beveiligingsrisico is verholpen, staan wij open voor overleg over eventuele publicatie van je bevindingen.

6. Safe harbor

Als je te goeder trouw handelt, binnen de grenzen van dit beleid blijft en je bevindingen zorgvuldig bij ons meldt, zullen wij geen juridische stappen tegen je ondernemen naar aanleiding van je melding.

Deze toezegging geldt niet wanneer sprake is van opzettelijke schade, misbruik, afpersing, datadiefstal, openbaarmaking zonder overleg, verstoring van systemen of ander handelen buiten de grenzen van dit beleid.

7. Publicatie

Publicatie over een beveiligingsrisico mag alleen plaatsvinden na overleg met Proxhost en nadat het beveiligingsrisico is verholpen, tenzij schriftelijk anders is afgesproken. Zo voorkomen we dat klanten, gebruikers of systemen onnodig risico lopen.

8. Geen beloningen

Wij bieden geen beloningen of bug bounties voor het melden van beveiligingsrisico's, tenzij hierover vooraf schriftelijk andere afspraken zijn gemaakt.

9. Contact

Beveiligingsmeldingen: security@proxhost.nl
Algemene contactgegevens: info@proxhost.nl