Coordinated Vulnerability Disclosure (CVD)

Onemeeting B.V.

Versie: 1.0 - Datum: 24 december 2025

Scope

onemeeting.com en subdomeinen die wij beheren.

Inleiding

Bij Onemeeting vinden we de veiligheid van onze systemen erg belangrijk. Ondanks alle beveiligingsmaatregelen die Onemeeting neemt, kan een zwakke plek voorkomen.
Kwetsbaarheid gevonden? Meld het direct bij ons. We beoordelen en verhelpen het zo snel en zorgvuldig mogelijk.
Dit is geen uitnodiging om uitgebreid te scannen of te testen; dat doen wij zelf.
Contact: security@onemeeting.com

Wat we je vragen

- Mail je bevindingen zo snel mogelijk naar security@onemeeting.com en voeg genoeg informatie toe om te reproduceren (URL/IP, beschrijving, stappen/PoC, impact, jouw contactgegevens).
- Misbruik de gevonden zwakheid niet: voer geen (D)DoS, brute-force, social engineering of malware-tests uit. Wijzig/verwijder geen data en exfiltreer geen persoonsgegevens.
- Deel details niet openbaar voordat er een oplossing beschikbaar is.

Wat wij beloven

- Wij sturen een ontvangstbevestiging binnen 3 werkdagen, met eerste inschatting en vervolgstappen.
- Transparante updates en een redelijke oplostermijn op basis van impact.
- De melding wordt vertrouwelijk behandeld en persoonlijke gegevens worden niet zonder toestemming met derden gedeeld, tenzij dat nodig is om een wettelijke verplichting na te komen. Safe harbor: handel je te goeder trouw volgens dit beleid, dan ondernemen wij geen juridische stappen.
- Vermelding (op verzoek) na oplossing.

Buiten scope

- Scanner-meldingen zonder analyse.
- Informatieve header/banner-leaks.
- Laag-risico “best practices”.
- Issues op systemen buiten ons beheer.