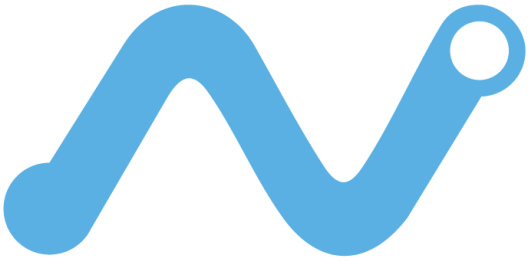
Polityka zgłaszania podatności (CVD)

dla produktów cyfrowych

marki



netberg

Chmielów, październik 2026

1. Cel polityki

Celem niniejszej Polityki Zgłaszania Podatności (Coordinated Vulnerability Disclosure Policy) jest zapewnienie bezpiecznego, przejrzystego i odpowiedzialnego procesu zgłaszania podatności dotyczących produktów cyfrowych marki **netberg.**
Polityka określa zasady kontaktu, obsługi zgłoszeń oraz współpracy z badaczami bezpieczeństwa, klientami i partnerami.

2. Zakres

Polityka dotyczy wszystkich produktów z elementami cyfrowymi oferowanych przez **MegaMarket S,A. w Chmielowie KRS:0000522574, NIP:8672239415, REGON: 181151371 (adres: ul. Strefowa 15, 39-442 Chmielów, Polska)** w tym:

- urządzeń IoT,
- oprogramowania wbudowanego (firmware),
- aplikacji mobilnych o ile są oferowane przez MegaMarket S.A. wraz z produktem,
- usług chmurowych o ile są oferowane przez MegaMarket S.A. wraz z produktem,
- interfejsów API i paneli administracyjnych o ile są oferowane przez MegaMarket S.A..

3. Kanał zgłaszania podatności

Zgłoszenia podatności należy kierować na dedykowany kanał bezpieczeństwa:

- **e-mail:** security@megamarket.pl
- **plik security.txt:** https://megamarket.pl/.well-known/security.txt

Kanał jest monitorowany i obsługiwany przez zespół bezpieczeństwa MegaMarket S.A.

4. Jak zgłaszać podatność

Prosimy o podanie następujących informacji (w miarę możliwości):

- opis podatności i jej potencjalnego wpływu,
- kroki potrzebne do odtworzenia problemu,
- informacje o środowisku (model urządzenia, wersja firmware, wersja aplikacji),
- PoC (Proof of Concept), jeśli jest dostępny,
- dane kontaktowe umożliwiające komunikację zwrotną.

5. Zasady odpowiedzialnego ujawniania

Prosimy badaczy o:

- niepublikowanie informacji o podatności przed zakończeniem procesu naprawy,
- unikanie działań powodujących szkody dla użytkowników, danych lub infrastruktury,
- nieuzyskiwanie nieautoryzowanego dostępu do danych użytkowników,
- nieprzeprowadzanie testów w środowisku produkcyjnym bez zgody.

6. Potwierdzenie i terminy

Po otrzymaniu zgłoszenia:

- **do 7 dni** – potwierdzamy odbiór zgłoszenia,
- **do 30 dni** – przekazujemy wstępną ocenę podatności,
- **do 90 dni** – dostarczamy poprawkę lub plan działań naprawczych (jeśli możliwe).

W przypadku podatności **aktywnie wykorzystywanej** lub o **wysokim ryzyku**, działania są podejmowane priorytetowo zgodnie z CRA.

7. Komunikacja i współpraca

Zobowiązujemy się do:

- utrzymywania kontaktu z badaczem,
- informowania o postępach prac,
- publikacji informacji o poprawkach bezpieczeństwa,

8. Ochrona zgłaszających

Badacze działający zgodnie z niniejszą polityką:

- nie będą traktowani jako osoby działające w złej wierze,
- nie będą podlegać działaniom prawnym, jeśli działali odpowiedzialnie i w dobrej wierze,

9. Zmiany polityki

Polityka może być aktualizowana w celu dostosowania do zmian prawnych (w tym CRA) oraz najlepszych praktyk bezpieczeństwa.

Zespół MegaMarket S.A.