ZAZ-En sp. z o.o.
ul. Marii Konopnickiej 13, 41-100 Siemianowice Śląskie
tel. +48 32 726 69 23, faks +48 32 494 48 85
biuro@zaz-en.pl, http://zaz-en.pl

Polityka ujawniania podatności (Coordinated Vulnerability Disclosure — CVD)

Data: 2026-09-01

1. Wprowadzenie

ZAZ-En sp. z o.o. produkuje urządzenia elektroenergetycznej automatyki zabezpieczeniowej z elementami cyfrowymi i interfejsami sieciowymi. Bezpieczeństwo naszych produktów i klientów traktujemy priorytetowo.

Zachęcamy badaczy bezpieczeństwa, partnerów i użytkowników do odpowiedzialnego zgłaszania potencjalnych podatności.

Polityka jest zgodna z Rozporządzeniem (UE) 2024/2847 (CRA) w zakresie obsługi podatności.

2. Zakres

Dotyczy podatności w:
- firmware i oprogramowaniu urządzeń serii iZAZ.
- oficjalnych narzędziach konfiguracyjnych ZAZ-En.

Nie dotyczy: infrastruktury należącej wyłącznie do klienta (sieć stacji, serwery klienta), chyba że podatność leży w produkcie ZAZ-En.

3. Jak zgłosić podatność

Preferowany kanał:
E-mail: security@zaz-en.pl

Alternatywnie: plik security.txt pod adresem https://zaz-en.pl/.well-known/security.txt

W zgłoszeniu prosimy o:

1. Opis podatności i kroki reprodukcji
2. Model urządzenia (np. iZAZ400) i wersję firmware (np. 260804)
3. Środowisko testowe
4. Potencjalny wpływ
5. Dane kontaktowe
6. Czy zgłoszenie jest poufne (domyślnie: tak)

Języki: polski, angielski.

4. Nasze zobowiązania

Potwierdzenie otrzymania — 2 dni robocze
Wstępna ocena — 5 dni roboczych
Plan remediacji — 30 dni (zależnie od złożoności)

Przy aktywnie wykorzystywanej podatności stosujemy obowiązki raportowania CRA (ENISA/CSIRT w terminach prawnych).

5. Safe harbor (dobra wiara)

Jeśli zgłaszający działa w dobrej wierze, nie narusza prywatności, nie eksfiltruje danych poza minimum potrzebne do demonstracji i daje rozsądny czas na poprawkę — ZAZ-En sp. z o.o. nie będzie inicjować postępowania prawnego za legalny test zgodny z niniejszą polityką.

Nie akceptujemy: ataków na systemy produkcyjne klientów bez zgody, szantażu, publicznego ujawnienia zero-day bez uprzedniego kontaktu.

6. Ujawnianie publiczne

Koordynowane ujawnienie — preferowany termin 90 dni od zgłoszenia (krócej przy aktywnej eksploatacji). Security Advisory z numerem wersji poprawki. Wymienienie zgłaszającego za zgodą.

7. Program nagród (bug bounty)

ZAZ-En sp. z o.o. nie prowadzi płatnego programu bug bounty.

8. Kontakt

E-mail PSIRT: security@zaz-en.pl
Serwis techniczny: serwis@zaz-en.pl
Telefon: +48 882 856 083
Polityka (URL): https://zaz-en.pl/pl/firma/cvd.html
security.txt: https://zaz-en.pl/.well-known/security.txt
Siedziba: ul. Marii Konopnickiej 13, 41-100 Siemianowice Śląskie, Polska

9. Zmiany polityki

Aktualna wersja na https://zaz-en.pl/pl/firma/cvd.html