

Polityka ujawniania podatności

Vulnerability Disclosure Policy — system ProfitEMS

Identyfikator	POL-SEC-004	Wersja	1.0
Klasyfikacja	Publiczny	Data zatwierdzenia	2026-08-12
Właściciel	Osoba odpowiedzialna za bezpieczeństwo (Security Officer)	Data wejścia w życie	2026-08-12
Zatwierdził	Zarząd PROFITEMS Sp. z o.o.	Cykl przeglądu	co 12 miesięcy

1. Nasze zobowiązanie

PROFITEMS Sp. z o.o. („Producent”) traktuje bezpieczeństwo systemu ProfitEMS — zarządzającego energią w domach klientów — jako warunek zaufania do produktu. Doceniamy pracę badaczy bezpieczeństwa, klientów i partnerów, którzy w dobrej wierze zgłaszają nam zauważone słabości. Zobowiązujemy się każde zgłoszenie przyjmując, przeanalizować i odpowiedzieć na nie w terminach opisanych w sekcji 7.

Polityka realizuje prowidę 5.2 normy ETSI EN 303 645 V3.1.3 (zarządzanie zgłoszeniami podatności), jest zgodna z wytycznymi ISO/IEC 29147 oraz stanowi przygotowanie do obowiązków zgłoszeniowych rozporządzenia CRA (2024/2847), obowiązujących od 11.09.2026. Jest opublikowana wraz z plikiem security.txt (RFC 9116) pod adresem <https://profitems.pl/.well-known/security.txt>.

2. Zakres

2.1 Komponenty objęte polityką

Komponent	Identyfikacja
Strona produktu i API usługi chmurowej	https://profitems.pl (HTTPS)
Panel instalatora / administratora i portal klienta	https://panel.profitems.pl (HTTPS)
Kanał komunikacji urządzeń z usługą chmurową	szyfrowany kanał TCP z uwierzytelnianiem urządzeń (Modbus TCP w tunelu TLS)
Bramka komunikacyjna EMS Connect	warstwa konfiguracji i tokenów urządzenia (dostarczana przez Producenta)
Aplikacja mobilna ProfitEMS	dystrybucja przez sklepy aplikacji

2.2 Poza zakresem

- Falowniki hybrydowe i magazyny energii (produkty ich producentów — zgłoszenia kierowane do producenta urządzenia).
- Infrastruktura Operatora Sieci Dystrybucyjnej, w tym liczniki energii.
- Sieć lokalna klienta (router, łącze internetowe).
- Warstwa sprzętowa modułu komunikacyjnego bramki jako produkt jego producenta — polityka obejmuje wyłącznie konfigurację i tokeny dostarczane przez ProfitEMS.

- Usługi podmiotów zewnętrznych zintegrowane z systemem (hosting, poczta transakcyjna) — zgłoszenia kierowane do tych podmiotów.

3. Zasady prowadzenia badań

Prosimy osoby badające bezpieczeństwo systemu o:

- niezwłoczne zgłoszenie podatności po jej wykryciu i niepogłębianie dostępu ponad minimum potrzebne do wykazania problemu,
- niekopiowanie, niemodyfikowanie i nieusuwanie danych innych użytkowników; jeżeli dostęp do cudzych danych okaże się możliwy — przerwanie testu i zgłoszenie,
- powstrzymanie się od działań obniżających dostępność usługi (ataki DoS/DDoS, masowe skanowanie z dużym wolumenem),
- powstrzymanie się od socjotechniki (phishing wobec pracowników, klientów lub partnerów) oraz od fizycznej ingerencji w urządzenia klientów (bramka, falownik, magazyn energii),
- niewykorzystywanie podatności komercyjnie i nieujawnianie jej osobom trzecim przed naprawą.

4. Bezpieczna przystań (Safe Harbor)

Badania prowadzone w dobrej wierze i zgodnie z niniejszą polityką uznajemy za działania upoważnione. Wobec osób przestrzegających zasad z sekcji 3 Producent:

- nie będzie inicjował postępowań cywilnych ani karnych w związku z prowadzonymi badaniami,
- a jeżeli postępowanie zainicjuje osoba trzecia — potwierdzi, że badacz działał zgodnie z opublikowaną polityką Producenta.

Ochrona nie obejmuje działań wykraczających poza zasady z sekcji 3, w szczególności: ataków na dostępność usługi, socjotechniki, fizycznej ingerencji w urządzenia klientów, eksfiltracji danych oraz modyfikacji ustawień sterowania instalacjami klientów.

5. Jakie zgłoszenia są szczególnie cenne

- naruszenia kontroli dostępu (dostęp do danych innego klienta lub innej firmy, eskalacja uprawnień),
- wstrzykiwanie kodu (SQL injection, XSS, wstrzykiwanie poleceń),
- słabości uwierzytelniania (sesje, tokeny urządzeń, odzyskiwanie hasła),
- manipulacja danymi kanału urządzeń prowadząca do zmiany harmonogramu sterowania,
- wycieki danych telemetrycznych lub osobowych,
- słabości kryptograficzne w przechowywaniu lub transmisji danych.

5.1 Zgłoszenia poza zakresem oceny

Nie traktujemy jako podatności m.in.: braku nagłówków „najlepszych praktyk” bez wykazanego wpływu, wyników automatycznych skanerów bez potwierdzenia możliwości wykorzystania, ataków wymagających ekstremalnego wolumenu ruchu, self-XSS wymagającego nietypowych działań użytkownika, braku zabezpieczeń poczty na domenach niesłużących do wysyłki oraz podatności w bibliotekach zewnętrznych bez wykazania ich wykorzystania w ProfitEMS.

6. Jak zgłosić podatność

Zgłoszenia przyjmujemy na adres: **security@profitems.pl** (adres potwierdzony w pliku security.txt). Preferowane języki: polski i angielski.

Aby przyspieszyć obsługę, prosimy o podanie: opisu podatności i jej potencjalnego wpływu, komponentu którego dotyczy (sekcja 2.1), kroków odtworzenia (proof of concept), minimalnych danych potwierdzających (żądanie/odpowiedź, zrzut ekranu), opcjonalnie sugerowanej oceny CVSS v3.1 oraz danych kontaktowych do dalszej korespondencji. Zgłoszenia anonimowe również przyjmujemy.

7. Czego może oczekiwać zgłaszający

Etap	Co robimy	Termin
Potwierdzenie przyjęcia	Potwierdzamy otrzymanie zgłoszenia i nadajemy mu identyfikator.	24 godziny
Ocena	Walidujemy zgłoszenie, oceniamy wagę (CVSS) i klasyfikujemy wg polityki reagowania na incydenty (P1–P4); przekazujemy plan naprawy.	72 godziny
Naprawa	P1 (CVSS 9.0–10.0) — do 24 h od oceny; P2 (7.0–8.9) — do 48 h; P3 (4.0–6.9) — do 7 dni; P4 — w cyklu wydań produktu.	wg klasy
Aktualizacja statusu	Do czasu naprawy informujemy zgłaszającego o postępie (przyjęte / w analizie / w naprawie / wdrożone).	co 14 dni
Zamknięcie	Informujemy o wdrożeniu poprawki i uzgadniamy ewentualną publikację.	po wdrożeniu

8. Skoordynowane ujawnianie

Stosujemy zasadę skoordynowanego ujawniania: zgłaszający może opublikować szczegóły podatności po upływie **90 dni** od zgłoszenia albo niezwłocznie po wydaniu poprawki — w zależności od tego, co nastąpi wcześniej — po uzgodnieniu zakresu publikacji z Producentem. Dla podatności krytycznych termin może zostać zmieniony za zgodą obu stron.

9. Podziękowania

Producent nie prowadzi obecnie programu premiowego (bug bounty). Za zgodą zgłaszającego publikujemy podziękowania na stronie produktu (imię lub pseudonim, data zgłoszenia, ogólna kategoria podatności — bez szczegółów technicznych).

10. Zgłoszenia do organów

Niezależnie od obsługi zgłoszenia, od 11.09.2026 Producent zgłasza aktywnie wykorzystywane podatności zgodnie z art. 14 rozporządzenia CRA (powiadomienie wstępne 24 h, szczegółowe 72 h, raport końcowy 14 dni) — procedurę określa Polityka reagowania na incydenty (POL-SEC-002).

11. Powiązane dokumenty

- Polityka reagowania na incydenty (POL-SEC-002)
- Polityka zarządzania ryzykiem (POL-SEC-001)
- Deklaracja Zgodności ProfitEMS

- security.txt — <https://profitems.pl/.well-known/security.txt> · opis dla zgłaszających:
<https://profitems.pl/bezpieczenstwo>

12. Historia wersji

Wersja	Data	Autor	Opis zmiany	Zatwierdził
1.0	2026-08-12	Security Officer	Pierwsze wydanie dokumentu	Zarząd

13. Zatwierdzenie

Niniejsza polityka została zatwierdzona przez Zarząd PROFITEMS Sp. z o.o. i obowiązuje od dnia wejścia w życie.



Mateusz Malec — Prezes Zarządu
data i podpis

PROFITEMS sp. z o.o.
ul.Kopernika 10, 87-200 Wąbrzeźno
tel. 881 042 386
~~KRS-0001253016~~
NIP 8781812492 REGON 545212556

Dokument realizuje prowidę 5.2 normy ETSI EN 303 645 V3.1.3 (2024-09), jest zgodny z wytycznymi ISO/IEC 29147 i RFC 9116 oraz przygotowuje wykonanie obowiązków z art. 14 rozporządzenia CRA (2024/2847) obowiązujących od 11.09.2026.