POLITYKA SKOORDYNOWANEGO UJAWNIANIA PODATNOŚCI POJAZDY SZYNOWE PESA BYDGOSZCZ S.A.

Wstęp i podstawa prawna

Celem niniejszej polityki jest ustanowienie zasad bezpiecznego zgłaszania, przyjmowania, analizy, koordynacji i ujawnienia informacji o podatnościach dotyczących produktów firmy Pojazdy Szynowe PESA Bydgoszcz S.A. Polityka ta definiuje procedury zarządzania podatnościami, zapewniając zgodność z „zasadniczymi wymaganiami" (essential requirements) określonymi w Załączniku I do rozporządzenia Cyber Resilience Act (CRA).

Niniejsza polityka stanowi fundament strategii bezpieczeństwa Pojazdy Szynowe PESA Bydgoszcz S.A., co oznacza pełne wdrożenie rygorów regulacyjnych przed końcem 2027 roku. Działania marki opierają się na międzynarodowych standardach, w szczególności na serii norm IEC 62443, co gwarantuje systemowe podejście do ochrony użytkowników i infrastruktury cyfrowej.

Zakres obowiązywania

Polityka obejmuje wszystkie „produkty z elementami cyfrowymi" (sprzęt i oprogramowanie z możliwością komunikacji) wprowadzane do obrotu pod marką PESA.

Procedura zgłaszania podatności

Wszelkie zidentyfikowane podatności należy zgłaszać bezpośrednio do Zespołu ds. Cyberbezpieczeństwa i/lub do CSIRT NASK. Pojazdy Szynowe PESA Bydgoszcz S.A. zobowiązuje się do niepodejmowania kroków prawnych przeciwko badaczom, którzy działają w dobrej wierze i przestrzegają zasad niniejszej polityki (Safe Harbor).

Adres e-mail: csirt@pesa.pl

Numer telefonu: +48 882 477 302

- Szyfrowanie: Ze względu na poufność danych, Pojazdy Szynowe PESA Bydgoszcz S.A. wymaga szyfrowania zgłoszeń (klucz PGP dostępny na żądanie).
- Potrzebne informacje:
  - Model urządzenia i numer seryjny.
  - Wersja oprogramowania układowego (firmware) lub aplikacji.
  - Szczegółowy opis techniczny i kroki do reprodukcji (PoC).
- Zasady bezpieczeństwa: Przyjmujemy wyłącznie opisy tekstowe i zrzuty ekranu w bezpiecznych formatach (PNG/JPG). Przesyłanie plików wykonywalnych jest zabronione.
- Dopuszczalne jest zgłoszenie anonimowe

Proces obsługi i koordynacji (PSIRT)

Za koordynację działań naprawczych odpowiada Zespół ds. Cyberbezpieczeństwa, działający według następującego schematu:

1. Potwierdzenie: Formalne potwierdzenie odbioru zgłoszenia w ciągu 48 godzin.
2. Weryfikacja i klasyfikacja: Ocena dotkliwości podatności przy użyciu systemu CVSS (Common Vulnerability Scoring System).
3. Opracowanie poprawki: Prace inżynieryjne nad nową wersją oprogramowania lub obejściem problemu (workaround).
4. Testowanie i publikacja: Weryfikacja skuteczności łatek i ich oficjalna dystrybucja.
5. Powiadomienie klienta: Publikacja oficjalnego ogłoszenia (Security Advisory)

Zobowiązania producenta w ramach CRA

Jako producent odpowiedzialny, PESA realizuje wymagania CRA poprzez:

• Raportowanie podatności: Aktywne zgłaszanie wykorzystanych podatności (exploited vulnerabilities) do ENISA w wymaganym czasie.

• Security-by-design: Stosowanie normy IEC 62443-4-1 w procesie rozwoju oraz zapewnienie funkcji bezpieczeństwa zgodnie z IEC 62443-4-2.

• Dokumentacja: Dostarczanie precyzyjnych instrukcji bezpiecznej konfiguracji i eksploatacji w celu minimalizacji ryzyka po stronie użytkownika.

Zasady współpracy (Safe Harbor)

Organizacja nie będzie inicjować działań prawnych wobec osób prowadzących badania w dobrej wierze i zgodnie z niniejszą polityką w zakresie pozostającym pod kontrolą PESA. Warunkiem zachowania statusu Safe Harbor jest przestrzeganie embarga informacyjnego w okresie do 90 dni od momentu zgłoszenia podatności do jej publicznego ujawnienia. W tym czasie badacz zobowiązany jest do zachowania poufności, co pozwala PESA na opracowanie i przetestowanie poprawki przed jej nagłośnieniem.

Dostępność aktualizacji i komunikacja

Oficjalne komunikaty bezpieczeństwa publikowane są w sekcji „Security Advisories" na stronie marki. W odniesieniu do produktów starszych (legacy), których specyfikacja sprzętowa nie pozwala na pełną zgodność z nowymi wymogami CRA, PESA zapewnia transparentność poprzez publikację „oświadczeń o zakończeniu wsparcia" (end-of-support statements) z odpowiednim wyprzedzeniem oraz oferowanie adekwatnych rozwiązań zamiennych.

Dane kontaktowe i administracyjne

Dedykowany kanał komunikacji w sprawach informowania o podatnościach:

E-mail: csirt@pesa.pl

telefon: +48 882 477 302