

SALUS Controls PLC - Formularz zgłoszenia podejrzenia podatności

Użyj tego formularza, aby zgłosić podejrzenie podatności bezpieczeństwa dotyczącej produktu SALUS, aplikacji, usługi chmurowej lub strony internetowej.

Prosimy o podanie jak największej ilości informacji. Nie musisz wypełniać wszystkich pól, abyśmy mogli przyjąć zgłoszenie.

Zgłoszenie można przesłać anonimowo. Jeśli jednak nie podasz danych kontaktowych, możemy nie mieć możliwości poproszenia o dodatkowe informacje ani przekazywania aktualizacji dotyczących zgłoszenia.

Po wypełnieniu formularza prosimy przesłać go na adres security@saluscontrols.com.

Prosimy nie zamieszczać haseł, tokenów uwierzytelniających, kluczy prywatnych ani zbędnych danych osobowych lub danych klientów.

Pola oznaczone jako „Wymagane” należy wypełnić tylko wtedy, gdy dane te są w rozsądnym zakresie dostępne. Zgłoszenie można przesłać również bez kompletu informacji.

Zgłoszenie podejrzenia podatności

1. Informacje o osobie zgłaszającej

Pole	Odpowiedź
Imię i nazwisko lub alias (opcjonalnie)	
Organizacja (opcjonalnie)	
E-mail / sposób kontaktu (wymagane, chyba że zgłoszenie jest anonimowe)	
Preferowany język (opcjonalnie)	
Zgłoszenie anonimowe?	☐ Tak ☐ Nie

2. Produkt lub komponent, którego dotyczy zgłoszenie

Pole	Odpowiedź
Nazwa produktu lub usługi (wymagane)	
Model (jeśli dotyczy)	
Wersja sprzętu (jeśli znana)	
Wersja firmware / oprogramowania / aplikacji (jeśli znana)	
Kraj / region	

Pole	Odpowiedź
Inne istotne informacje o konfiguracji	

3. Opis podejrzewanej podatności

Pole	Odpowiedź
Krótki tytuł (wymagane)	
Opisz zidentyfikowany problem bezpieczeństwa (wymagane)	
Kiedy po raz pierwszy zauważyłeś(-aś) problem?	
Jakiego działania oczekiwałeś(-aś)?	
Co faktycznie się wydarzyło?	
Czy możesz odtworzyć problem?	☐ Tak ☐ Nie ☐ Czasami ☐ Nie wiadomo ☐
Jeśli to możliwe, opisz kroki potrzebne do odtworzenia problemu:	
Jaki wpływ na bezpieczeństwo może mieć ten problem?	
Attachments included? You may provide relevant screenshots, logs, videos or proof-of-concept information.	☐ Tak ☐ Nie

Dodatkowe informacje techniczne (opcjonalnie - dla badaczy bezpieczeństwa)

Pole	Odpowiedź
Typ podatności (obejście uwierzytelniania, wstrzyknięcie, uszkodzenie pamięci itp.), jeśli znany	
CWE/ CVE, if known	
Przyczyna techniczna / szczegóły	
Środowisko testowe / konfiguracja	
Proof of concept	

4. Scenariusz ataku

Scenariusz ataku różni się od procedury odtworzenia problemu. Opisz, w jaki sposób rzeczywisty atakujący mógłby wykorzystać tę podatność.

Pole	Odpowiedź
Jeśli wiadomo, opisz, w jaki sposób ktoś mógłby wykorzystać tę podatność	
Dostęp atakującego	☐ Sieć zdalna ☐ Sieć sąsiednia ☐ Sieć lokalna ☐ Urządzenie lokalne ☐ Dostęp fizyczny ☐ Nie wiadomo
Wymagana interakcja użytkownika	☐ Tak ☐ Nie ☐ Nie wiadomo
Wymagane specjalne uprawnienia / konto	☐ Tak ☐ Nie ☐ Nie wiadomo Jeśli tak, opisz wymagane uprawnienia / konto:

5. Ocena wpływu (opcjonalnie)

Wypełnij tę sekcję, jeśli możesz ocenić potencjalny wpływ.

Obszar wpływu	Ocena osoby zgłaszającej
Poufność	☐ Brak ☐ Niski ☐ Średni ☐ Wysoki ☐ Nie wiadomo ☐ ☐ ☐ ☐
Integralność	☐ Brak ☐ Niski ☐ Średni ☐ Wysoki ☐ Nie wiadomo ☐ ☐ ☐ ☐
Dostępność	☐ Brak ☐ Niski ☐ Średni ☐ Wysoki ☐ Nie wiadomo ☐ ☒ ☐ ☐
Bezpieczeństwo fizyczne	☐ Brak ☐ Niski ☐ Średni ☐ Wysoki ☐ Nie wiadomo ☐ ☐ ☐ ☐
Prywatność	☐ Brak ☐ Niski ☐ Średni ☐ Wysoki ☐ Nie wiadomo ☐ ☐ ☐ ☐
Wpływ na łańcuch dostaw lub szerszy ekosystem	☐ Brak ☐ Niski ☐ Średni ☐ Wysoki ☐ Nie wiadomo
Sugerowany poziom ważności, jeśli dostępny (opcjonalnie)	☐ Niski ☐ Średni ☐ Wysoki ☐ Krytyczny ☐ Nie wiadomo
Wektor CVSS, jeśli dostępny (opcjonalnie)	

6. Status wykorzystania podatności i ujawnienia

Pole	Odpowiedź
Czy podatność jest już publicznie znana?	☐ Nie ☐ Tak ☐ Nie wiadomo Jeśli tak, podaj adres URL i datę:
Czy proof of concept jest publicznie dostępny?	☐ Nie ☐ Tak ☐ Nie wiadomo Jeśli tak, podaj adres URL i datę:
Czy wiadomo o aktywnym wykorzystywaniu podatności lub jest ono podejrzewane?	☐ Nie ☐ Tak ☐ Nie wiadomo Jeśli tak, podaj szczegóły:
Czy skontaktowano się z innym producentem, dostawcą, zespołem CERT lub koordynatorem?	☐ Nie ☐ Tak ☐ Nie wiadomo Jeśli tak, podaj podmiot, identyfikator sprawy i datę:
Czy planujesz omówić lub opublikować informacje o problemie po jego usunięciu?	☐ Nie ☐ Tak ☐ Nie wiadomo Jeśli tak, podaj szczegóły:
Preferowana data skoordynowanego ujawnienia, jeśli dotyczy	

Informacja dotycząca skoordynowanego ujawnienia: Prosimy zachować poufność niepublicznych informacji o podatności do uzgodnionej daty ujawnienia. Jeśli poziom ryzyka ulegnie zmianie, zostanie zaobserwowane aktywne wykorzystywanie podatności lub publiczne ujawnienie stanie się prawdopodobne, prosimy niezwłocznie skontaktować się z **security@saluscontrols.com**, aby można było ponownie ocenić plan ujawnienia.

7. Sugerowane działania naprawcze lub ograniczające ryzyko (opcjonalnie)

- Sugerowana poprawka usuwająca przyczynę źródłową, jeśli jest znana: _____
- Sugerowane tymczasowe ograniczenie ryzyka lub obejście problemu, jeśli jest znane: _____
- Odpowiednia praktyka branżowa, reguła ochronna lub odniesienie: _____

8. Preferencje dotyczące podziękowania

Wybór	Odpowiedź
Czy możemy publicznie podziękować Ci w przypadku opublikowania komunikatu?	☐ Tak ☐ Nie
Nazwa wyświetlana, alias lub organizacja	
Preferowany profil lub link referencyjny, jeśli jest zgodny z polityką	

9. Załączniki i dodatkowe informacje

Prosimy wymienić wszystkie pliki dołączone do zgłoszenia. Nie należy dołączać haseł, tokenów uwierzytelniających, kluczy prywatnych ani zbędnych danych osobowych lub danych klientów.

Pole	Odpowiedź
Czy do zgłoszenia dołączono pliki?	☐ Tak ☐ Nie
Rodzaj dołączonych plików	☐ Zrzuty ekranu ☐ Logi ☐ Wideo ☐ Proof of concept ☐ Przechwycone pakiety ☐ Inne
Opis dołączonych plików	
Dodatkowe informacje istotne dla zgłoszenia	
Wymagania dotyczące poufności lub sposobu postępowania	

Jeśli dołączasz logi, zrzuty ekranu, nagrania wideo, przechwycone pakiety lub materiały typu proof of concept, przed przesłaniem zgłoszenia usuń zbędne dane osobowe, dane klientów, hasła, tokeny uwierzytelniające, klucze prywatne oraz inne informacje wrażliwe.

10. Oświadczenie o działaniu w dobrej wierze

Przesyłając to zgłoszenie, osoba zgłaszająca potwierdza, zgodnie ze swoją najlepszą wiedzą, że:

- ☐ Zgłoszenie jest zgodne ze stanem faktycznym i powstało w wyniku badań bezpieczeństwa prowadzonych w dobrej wierze.
- ☐ Testy ograniczały się do systemów, urządzeń, kont i danych należących do osoby zgłaszającej lub takich, do których testowania była upoważniona.
- ☐ Unikano zbędnego dostępu do niepublicznych danych, ich przechowywania lub ujawniania.
- ☐ Osoba zgłaszająca będzie koordynować ujawnienie zgodnie z opublikowaną polityką, z zastrzeżeniem obowiązującego prawa oraz wszelkich pilnych zmian poziomu ryzyka dla użytkowników.
- ☐ Potwierdzam, że celowo nie zamieściłem(-am) haseł, tokenów uwierzytelniających, kluczy prywatnych ani zbędnych danych osobowych lub danych klientów.

Data zgłoszenia: _____

Imię i nazwisko lub alias osoby zgłaszającej, jeśli podano:

Jak przesłać zgłoszenie

Wypełniony formularz prosimy przesłać e-mailem na adres: security@saluscontrols.com
 Podejrzanie podatności można również zgłosić bezpośrednio e-mailem, bez korzystania z tego formularza. Zalecamy jednak użycie formularza, ponieważ pomaga on SALUS Controls PLC zebrać informacje potrzebne do sprawnej oceny zgłoszenia.