Polityka ujawniania podatności

Odpowiedzialne zgłaszanie, badanie i usuwanie podatności bezpieczeństwa

Wersja	Data wejścia w życie	Właściciel dokumentu	Kontakt
1.0	Wrzesień 2026	Zespół ds. bezpieczeństwa SALUS Controls PLC	security@saluscontrols.com

1. Wprowadzenie

SALUS Controls PLC dba o bezpieczeństwo swoich produktów, usług i klientów. Zachęcamy klientów, badaczy bezpieczeństwa, partnerów, programistów i innych członków społeczności bezpieczeństwa do odpowiedzialnego zgłaszania potencjalnych podatności dotyczących produktów lub usług SALUS Controls PLC.

Naszym celem jest szybkie analizowanie zgłoszeń potencjalnych podatności, odpowiednia komunikacja ze zgłaszającym na każdym etapie oraz wdrażanie proporcjonalnych działań naprawczych lub ograniczających ryzyko w celu ochrony użytkowników.

Potencjalne podatności bezpieczeństwa należy zgłaszać poufnie na adres **security@saluscontrols.com**. SALUS Controls PLC potwierdzi odbiór w ciągu trzech dni roboczych, a w każdym przypadku nie później niż w ciągu siedmiu dni kalendarzowych. To potwierdzenie jedynie potwierdza otrzymanie informacji i nie oznacza, że zgłoszony problem został potwierdzony jako podatność.

2. Zakres

Niniejsza polityka ma zastosowanie do podatności bezpieczeństwa dotyczących:

- produktów SALUS Controls PLC
- oprogramowania układowego i oprogramowania
- aplikacji mobilnych
- usług chmurowych
- publicznie dostępnych aplikacji internetowych i stron WWW

W sprawach dotyczących instalacji, konfiguracji, gwarancji lub innych kwestii niezwiązanych z bezpieczeństwem prosimy kontaktować się z naszym zespołem obsługi klienta za pośrednictwem standardowych kanałów wsparcia.

Przyjmujemy zgłoszenia dotyczące bezpieczeństwa produktów SALUS niezależnie od etapu ich cyklu życia. W przypadku produktów objętych opublikowanym okresem wsparcia bezpieczeństwa podatności i aktualizacje bezpieczeństwa są obsługiwane zgodnie z obowiązującymi wymogami prawnymi. Zgłoszenia dotyczące produktów poza tym okresem również będą oceniane przez SALUS Controls PLC; zależnie od ryzyka, wykonalności technicznej i obowiązujących wymogów możemy przedstawić środki ograniczające ryzyko, zalecenia migracyjne lub inne wskazówki.

3. Zgłaszanie podatności

Jeśli uważasz, że wykryłeś podatność bezpieczeństwa, zgłoś ją poufnie, wysyłając wiadomość na adres **security@saluscontrols.com**.

Zgłoszenia mogą być anonimowe. Brak imienia lub dwustronnego kanału kontaktu nie uniemożliwia przyjęcia ani wstępnej oceny zgłoszenia, ale może ograniczyć możliwość uzyskania dodatkowych informacji, przekazywania aktualizacji statusu lub publicznego uznania zgłaszającego.

Przyjmujemy zgłoszenia wstępne przesłane zwykłą pocztą elektroniczną lub innym kanałem. Jeżeli konieczna jest wymiana kodu exploitów, danych uwierzytelniających, danych osobowych, konfiguracji klientów lub innych informacji wrażliwych, SALUS Controls PLC zaproponuje dostępny bezpieczny sposób dalszej komunikacji. Brak możliwości użycia szyfrowania lub decyzja zgłaszającego o jego nieużywaniu nie będzie sama w sobie podstawą odrzucenia zgłoszenia.

4. Informacje, które należy podać

Aby umożliwić sprawne zbadanie zgłoszenia, prosimy w miarę możliwości podać:

- nazwę i model produktu
- wersję oprogramowania układowego lub oprogramowania
- opis podatności
- kroki wymagane do odtworzenia problemu
- oczekiwane i rzeczywiste zachowanie
- potencjalny wpływ na bezpieczeństwo
- zrzuty ekranu, logi lub proof-of-concept, jeśli są dostępne
- preferowane dane kontaktowe do dalszej komunikacji

Prosimy unikać przekazywania wrażliwych danych osobowych, chyba że są one niezbędne do wykazania podatności.

Jeśli wiadomo, prosimy również wskazać, czy problem jest publicznie znany, aktywnie wykorzystywany, wpłynął na użytkowników lub został zgłoszony innemu dostawcy, producentowi bądź koordynatorowi. Nie musisz podawać wszystkich wskazanych informacji, abyśmy mogli przyjąć i zarejestrować zgłoszenie.

W trakcie skoordynowanego ujawniania dostęp do niepublicznych informacji o podatności jest ograniczony do osób, które muszą je znać. SALUS Controls PLC może udostępniać niezbędne informacje zespołom produktowym, dostawcom, koordynatorom, stronom dotkniętym problemem lub właściwym organom w celu weryfikacji, usunięcia podatności, ochrony użytkowników i spełnienia obowiązków prawnych, z zachowaniem odpowiednich zasad poufności i ochrony danych.

Dane osobowe przekazane wraz ze zgłoszeniem podatności są przetwarzane zgodnie z właściwą polityką prywatności SALUS Controls PLC. Zobacz politykę prywatności: https://saluscontrols.com/pl/polityka-prywatnosci-cookie/.

5. Proces obsługi zgłoszenia

Po otrzymaniu zgłoszenia SALUS Controls PLC:

- potwierdzi odbiór w ciągu trzech dni roboczych, a w każdym przypadku nie później niż w ciągu siedmiu dni kalendarzowych; w miarę możliwości poda unikalny identyfikator sprawy i wstępny status.
- przeprowadzi wstępną ocenę w ciągu siedmiu dni roboczych
- zweryfikuje zgłoszoną podatność
- oceni jej dotkliwość i potencjalny wpływ
- opracuje plan naprawczy lub aktualizację bezpieczeństwa, jeśli będzie to zasadne
- będzie informować o przebiegu analizy i działań naprawczych
- dopóki sprawa pozostaje aktywna, przekaże merytoryczną aktualizację statusu co najmniej raz na 30 dni kalendarzowych, a wcześniej, jeśli istotnie zmieni się potwierdzony zakres, ryzyko, sposób naprawy lub termin ujawnienia.
- Jeśli potrzebne będą dodatkowe informacje, możemy skontaktować się z Tobą w trakcie analizy.

6. Usuwanie podatności w oparciu o ryzyko

Potwierdzone podatności są priorytetyzowane według dotkliwości technicznej, możliwości wykorzystania, dotkniętych produktów, potencjalnego wpływu, narażenia użytkowników, oznak aktywnego wykorzystania, dostępnych środków ograniczających ryzyko oraz wymagań bezpiecznego wdrożenia. Wynik punktowy może wspierać ocenę, ale sam nie wyznacza priorytetu działań naprawczych.

SALUS Controls PLC wyznacza dla każdej sprawy docelowy termin działań naprawczych i informuje zgłaszającego o istotnych zmianach. Jeśli natychmiastowa naprawa nie jest możliwa, przed udostępnieniem trwałego rozwiązania mogą zostać przekazane odpowiednie środki ograniczające ryzyko lub zalecenia jego redukcji.

7. Skoordynowane ujawnianie podatności

SALUS Controls PLC współpracuje ze zgłaszającym oraz, w razie potrzeby, z dostawcami, koordynatorami i innymi zainteresowanymi stronami w celu ustalenia terminu ujawnienia właściwego dla danej sprawy. Termin może zostać zmieniony zależnie od dotkliwości, aktywnego wykorzystania, ryzyka dla użytkowników, postępu napraw i wdrożenia, zależności w łańcuchu dostaw oraz obowiązków prawnych lub regulacyjnych. Istotne zmiany terminu będą przekazywane odpowiednim stronom.

SALUS Controls PLC może przyspieszyć powiadomienie użytkowników lub publiczne ujawnienie, jeśli podatność jest już publiczna, jest aktywnie wykorzystywana, stwarza pilne ryzyko dla użytkowników, istnieje prawdopodobieństwo jej wycieku lub prawo wymaga powiadomienia. Jeśli pełna poprawka nie jest jeszcze dostępna, SALUS może przekazać tymczasowe środki ograniczające ryzyko lub zalecenia bez zbędnego ułatwiania wykorzystania podatności.

Informacje o usuniętych podatnościach będą publikowane w dostępnych, czytelnych dla człowieka komunikatach bezpieczeństwa. Komunikaty będą określać podatność i dotknięte produkty, daty publikacji i zmian, potencjalny wpływ i dotkliwość, dostępne działania naprawcze lub ograniczające ryzyko, wymagane działania użytkownika oraz dane kontaktowe. W przypadku komponentów stron trzecich komunikaty mogą odsyłać do wiarygodnych źródeł producenta, jeśli pozwala to ustalić, czy problem dotyczy produktów SALUS.

Informacje o podatności będą również udostępniane w powszechnie uznanym formacie do odczytu maszynowego, chyba że udokumentowano i zatwierdzono uzasadnienie odstąpienia od tego wymogu. Publikacja może zostać opóźniona lub pominięta wyłącznie wtedy, gdy odpowiednie warunki zostały ocenione, udokumentowane i zatwierdzone.

Jeżeli wymaga tego prawo lub jest to konieczne dla ochrony użytkowników, SALUS Controls PLC poinformuje dotkniętych użytkowników i przekaże dostępne zalecenia ograniczające ryzyko lub działania korygujące za pośrednictwem odpowiednich, dostępnych kanałów.

8. Wsparcie aktualizacji bezpieczeństwa

SALUS Controls PLC zapewnia aktualizacje bezpieczeństwa przez cały okres wsparcia ustalony dla danego produktu. Okres wsparcia jest określany zgodnie z obowiązującymi wymogami prawnymi, z uwzględnieniem przewidywanego okresu użytkowania produktu, jego charakteru oraz uzasadnionych oczekiwań użytkowników.

Okres wsparcia wynosi co najmniej pięć lat, chyba że można zasadnie oczekiwać krótszego okresu użytkowania produktu, i może być dłuższy, jeśli uzasadnia to przewidywana żywotność produktu. Data zakończenia właściwego okresu wsparcia zostanie podana w odpowiednich informacjach o produkcie.

9. Poza zakresem

Wszystkie potencjalne zgłoszenia dotyczące bezpieczeństwa są rejestrowane i podlegają wstępnej ocenie. Kwestie wyłącznie funkcjonalne, handlowe lub związane ze wsparciem mogą zostać przekierowane do odpowiedniego kanału obsługi. Jeśli problemu początkowo nie można odtworzyć, SALUS Controls PLC może poprosić o dodatkowe informacje i ponownie ocenić zgłoszenie po uzyskaniu nowych dowodów.

Problemy teoretyczne, scenariusze wymagające fizycznego dostępu, warunki odmowy usługi, scenariusze socjotechniczne i zależności od stron trzecich są oceniane pod kątem rzeczywistego wpływu na bezpieczeństwo, możliwości wykorzystania oraz zamierzonego i racjonalnie przewidywalnego sposobu użycia produktu.

Podatności w komponentach stron trzecich zintegrowanych z produktem SALUS, dostarczanych wraz z nim lub wykorzystywanych przez niego nadal podlegają ocenie wpływu na produkt SALUS.

10. Odpowiedzialne badania bezpieczeństwa

SALUS Controls PLC wspiera odpowiedzialne badania bezpieczeństwa prowadzone w dobrej wierze. Prosimy badaczy, aby:

- działali odpowiedzialnie i etycznie
- nie zakłócali działania produktów, usług ani działalności klientów
- nie uzyskiwali dostępu do danych klientów, nie modyfikowali ich ani nie usuwali
- zgłaszali podatności poufnie zgodnie z procesem opisanym w niniejszej polityce
- zapewnili SALUS Controls PLC rozsądny czas na zbadanie i usunięcie problemu przed publicznym ujawnieniem
- podczas badań przestrzegali wszystkich obowiązujących przepisów prawa i regulacji

Jeśli zgłaszający działa w dobrej wierze, przestrzega niniejszej polityki, unika wyrządzania szkód i niezwłocznie dokonuje zgłoszenia, SALUS Controls PLC nie zamierza podejmować działań prawnych wyłącznie z powodu badań bezpieczeństwa przeprowadzonych zgodnie z tą polityką. Niniejsze oświadczenie nie upoważnia do uzyskiwania dostępu do systemów lub danych stron trzecich, nie wiąże stron trzecich ani organów i nie zwalnia zgłaszającego z obowiązku przestrzegania prawa oraz uzyskania wymaganych zezwoleń.

11. Kontakt

W sprawie wszystkich zgłoszeń dotyczących bezpieczeństwa lub pytań o niniejszą politykę prosimy o kontakt:

Zespół ds. bezpieczeństwa SALUS Controls PLC

E-mail: security@saluscontrols.com

12. Aktualizacje polityki

Niniejsza polityka jest przeglądana co najmniej raz w roku oraz po istotnych zmianach obowiązujących wymogów prawnych, kanałów zgłaszania, zakresu produktów lub procesów obsługi podatności. Aktualna wersja, data publikacji, data ostatniej aktualizacji i właściciel polityki są podawane wraz z opublikowaną polityką.

13. Uznanie autorstwa

Za zgodą zgłaszającego SALUS Controls PLC może publicznie wskazać imię, pseudonim lub organizację zgłaszającego, który przekazał prawidłowe zgłoszenie podatności i wspiera skoordynowane ujawnienie. Zgłoszenia mogą być anonimowe, a odmowa uznania autorstwa nie wpływa na przyjęcie, priorytetyzację ani decyzje dotyczące działań naprawczych.

Niniejsza polityka nie ustanawia programu bug bounty ani nie gwarantuje nagród finansowych lub innych.