

Polityka skoordynowanego ujawniania luk w zabezpieczeniach

Odpowiedzialne zgłaszanie luk w cyberbezpieczeństwie

Firma Otto Martin Maschinenbau GmbH & Co. KG („MARTIN”) przywiązuje dużą wagę do bezpieczeństwa swoich maszyn, oprogramowania i komponentów cyfrowych.

Pomimo starannego opracowania i testowania w produktach zawierających elementy cyfrowe mogą wystąpić luki w cyberbezpieczeństwie. Dlatego z zadowoleniem przyjmujemy zgłoszenia dotyczące potencjalnych luk od klientów, dystrybutorów, partnerów, badaczy zajmujących się bezpieczeństwem oraz innych osób.

W niniejszej Polityce skoordynowanego ujawniania luk w zabezpieczeniach (polityka CVD) opisujemy, w jaki sposób można zgłaszać firmie MARTIN potencjalne luki w cyberbezpieczeństwie oraz w jaki sposób postępujemy z otrzymanymi zgłoszeniami.

1. Zakres obowiązywania

Niniejsza polityka dotyczy luk w cyberbezpieczeństwie występujących w produktach i komponentach cyfrowych firmy MARTIN, w szczególności w:

- sterownikach maszyn,
- oprogramowaniu sterującym,
- oprogramowaniu układowym,
- interfejsach użytkownika,
- interfejsach sieciowych i komunikacyjnych,
- aplikacje internetowe i chmurowe, o ile stanowią one część produktu MARTIN lub są niezbędne do jego działania,
- aplikacje mobilne, o ile są dostępne,
- interfejsy i API, a także
- zintegrowane przez firmę MARTIN komponenty oprogramowania innych producentów.

Niniejsza polityka CVD nie obejmuje ogólnych reklamacji dotyczących produktów, usterek mechanicznych, pytań dotyczących obsługi ani innych zgłoszeń serwisowych niezwiązanych z cyberbezpieczeństwem. W tym celu prosimy o skorzystanie z naszych standardowych kanałów serwisowych i kontaktowych.

2. Zgłaszanie luk w zabezpieczeniach

Jeśli wykryją Państwo potencjalną lukę w cyberbezpieczeństwie w produkcie firmy MARTIN, prosimy o jak najszybsze poinformowanie nas o tym.

Centralny punkt kontaktowy ds. luk w cyberbezpieczeństwie

Otto Martin Maschinenbau GmbH & Co. KG

E-mail: product-security@martin.info

Formularz zgłoszeniowy online: <https://martin.info/pl/bezpieczenstwo-produktow/>

W przypadku informacji poufnych lub wrażliwych pod względem technicznym prosimy o korzystanie przede wszystkim z przeznaczonego do tego celu kanału przekazywania danych:

3. Jakie informacje są nam potrzebne?

Abyśmy mogli jak najszybciej sprawdzić zgłoszenie, prosimy o podanie następujących informacji – o ile są one znane i dostępne:

- produkt lub typ maszyny, którego dotyczy zgłoszenie,
- numer seryjny produktu,
- wersja oprogramowania lub oprogramowania układowego,
- dotyczy to konkretnego komponentu lub funkcji,
- opis domniemanej luki w zabezpieczeniach,
- możliwe skutki luki w zabezpieczeniach,
- kroki pozwalające odtworzyć to zachowanie,
- zastosowana konfiguracja sieciowa lub systemowa,
- w razie potrzeby zrzuty ekranu, pliki dziennika lub inne dowody techniczne,
- informacja o tym, czy luka jest już znana osobom trzecim lub została upubliczniona,
- informacja o tym, czy istnieją przesłanki wskazujące na aktywne wykorzystywanie luki,
- Państwa dane kontaktowe na wypadek pytań.

Prosimy nie przekazywać danych osobowych, danych dostępowych, tajemnic handlowych ani danych osób trzecich, o ile nie są one niezbędne do zbadania luki w zabezpieczeniach.

4. Co dzieje się po zgłoszeniu?

Po otrzymaniu zgłoszenia luki w zabezpieczeniach firma MARTIN rozpatrzy je w ramach ustalonego procesu zarządzania lukami w zabezpieczeniach.

Proces ten zasadniczo obejmuje następujące etapy:

1. Potwierdzenie odbioru: W odpowiednim terminie potwierdzimy otrzymanie zgłoszenia.
2. Wstępna ocena: Sprawdzamy, czy zgłoszenie dotyczy potencjalnej luki w cyberbezpieczeństwie produktu firmy MARTIN.
3. Analiza techniczna: Odpowiednie działy specjalistyczne badają lukę i oceniają w szczególności jej skutki techniczne, możliwość wykorzystania oraz wynikające z niej ryzyko.
4. Ustalanie priorytetów: Dalsze działania zależą od stopnia ważności, możliwości wykorzystania oraz potencjalnych skutków luki.
5. Działania naprawcze: W razie potrzeby i o ile jest to technicznie możliwe, opracowujemy odpowiednie środki mające na celu usunięcie lub ograniczenie ryzyka. Mogą to być na przykład aktualizacje oprogramowania lub oprogramowania układowego, zmiany konfiguracji, techniczne środki ochronne lub zalecenia dotyczące postępowania.
6. Skoordynowane ujawnienie: Ujawnienie szczegółów technicznych powinno zasadniczo nastąpić dopiero wtedy, gdy dostępne są odpowiednie środki zaradcze lub gdy skoordynowane ujawnienie jest uzasadnione lub konieczne z innych powodów.
7. Informowanie użytkowników, których dotyczy problem: W razie potrzeby informujemy klientów, sprzedawców lub użytkowników, których dotyczy problem, o odpowiednich środkach zaradczych i wskazówkach dotyczących bezpieczeństwa.

Nie ma to wpływu na ustawowe obowiązki zgłaszania i informowania, w szczególności wynikające z ustawy o cyberodporności (Cyber Resilience Act).

5. Skoordynowane ujawnianie informacji

Prosimy osoby zgłaszające o zapewnienie firmie MARTIN odpowiedniej możliwości zbadania i usunięcia luki w zabezpieczeniach, zanim szczegóły techniczne zostaną upublicznione lub przekazane osobom trzecim.

Konkretny termin zostanie uzgodniony między firmą MARTIN a zgłaszającym w zależności od rodzaju, złożoności i stopnia zagrożenia luki.

Ujawnienie informacji powinno być w szczególności skoordynowane w taki sposób, aby użytkownicy, których to dotyczy, mieli wystarczającą możliwość wdrożenia dostępnych aktualizacji zabezpieczeń lub innych środków ochronnych.

Jeśli luka jest już aktywnie wykorzystywana lub stanowi bezpośrednie, poważne zagrożenie, może być konieczna procedura przyspieszona.

6. Oczekiwania wobec badaczy bezpieczeństwa i osób zgłaszających

Prosimy o odpowiedzialne podejście podczas badania potencjalnych luk w zabezpieczeniach.

W szczególności prosimy o

- badania wyłącznie systemów i produktów, do których mają Państwo uprawnienia,
- nie przeglądać, nie zmieniać ani nie usuwać danych innych osób lub firm bez upoważnienia,
- nie stosowali złośliwego oprogramowania,
- nie podejmować działań, które zakłócałyby normalne działanie maszyn, systemów informatycznych lub sieci,
- nie przeprowadzać ataków typu „denial-of-service” ani podobnych testów obciążeniowych na systemach produkcyjnych,
- nie przeprowadzać ataków socjotechnicznych na pracowników, klientów, dystrybutorów lub partnerów biznesowych firmy MARTIN,
- nie wykorzystywać wykrytych luk w zabezpieczeniach w stopniu wykraczającym poza zakres niezbędny do weryfikacji,
- traktować uzyskane informacje jako poufne oraz
- zapewnić firmie MARTIN odpowiednią możliwość zbadania i usunięcia wykrytych problemów przed opublikowaniem szczegółów technicznych.

W przypadku maszyn i urządzeń badania nie mogą w żadnym wypadku prowadzić do wyłączenia funkcji zabezpieczających ani do narażenia osób, maszyn, obrabianych elementów lub innego mienia na niebezpieczeństwo.

7. Komunikacja z zgłaszającym

O ile udostępnią Państwo nam swoje dane kontaktowe, dołożymy starań, aby na bieżąco informować Państwa o istotnych postępach w trakcie badania.

Możemy skontaktować się z Państwem w szczególności, gdy:

- potrzebne będą dodatkowe informacje techniczne,
- udało się odtworzyć lukę w zabezpieczeniach,
- opracowano środek zaradczy lub
- planowane jest skoordynowane ogłoszenie wyników.

Prosimy pamiętać, że ze względów bezpieczeństwa, ochrony danych lub poufności możemy nie być w stanie ujawnić wszystkich wyników wewnętrznego dochodzenia.

8. Uznanie

Firma MARTIN z zadowoleniem przyjmuje zgłoszenia luk w cyberbezpieczeństwie dokonane w sposób odpowiedzialny.

Publiczne wymienienie zgłaszającego może nastąpić po wcześniejszym uzgodnieniu, o ile jest to pożądane i nie stoją temu na przeszkodzie żadne względy prawne, związane z bezpieczeństwem lub umowie.

Niniejsza polityka CVD nie daje prawa do wynagrodzenia finansowego ani innych nagród za zgłoszone luki w zabezpieczeniach.

9. Zgłoszenia wymagane prawem

Niezależnie od komunikacji z osobą zgłaszającą, firma MARTIN sprawdza w przypadku każdej istotnej luki, czy istnieją ustawowe obowiązki zgłoszeniowe lub informacyjne.

Dotyczy to w szczególności aktywnie wykorzystywanych luk w zabezpieczeniach oraz poważnych incydentów związanych z bezpieczeństwem w zakresie stosowania rozporządzenia (UE) 2024/2847 – Cyber Resilience Act (CRA).

W razie potrzeby odpowiednie zgłoszenia są kierowane do właściwych organów wyznaczonych do tego celu.

10. Ochrona danych

Dane osobowe przekazane nam w związku ze zgłoszeniem luki w zabezpieczeniach przetwarzamy wyłącznie w zakresie niezbędnym do rozpatrzenia, udokumentowania i śledzenia zgłoszenia, a także w celu wypełnienia obowiązków ustawowych.

Więcej informacji na temat ochrony danych można znaleźć pod adresem:

[Link do polityki prywatności]

11. Zmiany niniejszej polityki

Niniejsza Polityka skoordynowanego ujawniania luk w zabezpieczeniach jest regularnie weryfikowana i w razie potrzeby dostosowywana do zmian technicznych, organizacyjnych lub prawnych.

Stan na: 09/2026

Otto Martin Maschinenbau GmbH & Co. KG

Langenberger Str. 6

87724 Ottobeuren

Niemcy

Kontakt w sprawie bezpieczeństwa produktów: product-security@martin.info

Strona internetowa: www.martin.info