Polityka zgłaszania i obsługi podatności bezpieczeństwa

Bezpieczeństwo naszych rozwiązań — od systemów łączności radiowej po oprogramowanie dyspozytorskie i rozwiązania dla transportu szynowego — traktujemy priorytetowo. Poniższy dokument opisuje, w jaki sposób przyjmujemy, oceniamy i obsługujemy zgłoszenia o podatnościach dotyczących naszych produktów i infrastruktury, oraz na jakich zasadach współpracujemy z osobami je zgłaszającymi.

Do kogo i czego odnosi się ta polityka

Dokument obejmuje wszystkie oferowane przez Aksel Sp. z o.o. produkty i usługi zawierające elementy cyfrowe — niezależnie od tego, czy zostały przez nas opracowane, czy jedynie są przez nas utrzymywane lub eksploatowane — a także infrastrukturę firmową, do której zgłoszenia trafiają oficjalnymi kanałami wskazanymi poniżej.
Poza jego zakresem pozostają natomiast:

- rozwiązania i usługi dostawców zewnętrznych, których Aksel Sp. z o.o. nie jest właścicielem ani administratorem,
- sytuacje wynikające z indywidualnej konfiguracji u klienta lub z nieprawidłowego korzystania z produktu.

Kiedy zgłoszenie uznajemy za zasadną podatność

Przy kwalifikacji zgłoszenia jako ważnej podatności kierujemy się trzema kryteriami:

- zgłaszany problem musi dotyczyć konkretnego produktu lub elementu infrastruktury Aksel Sp. z o.o.,
- zgłoszenie powinno wskazywać na informacje, które nie są powszechnie znane,
- nie może ono opierać się wyłącznie na wyniku automatycznego skanu bez dołączonej dokumentacji — podatność musi dawać się faktycznie wykorzystać w warunkach rzeczywistej eksploatacji.

Jak zgłosić podatność

Zgłoszenia przyjmujemy przez dedykowany, bezpieczny kanał:

E-mail: cybersecurity@aksel.com.pl
Formularz kontaktowy:
https://www.aksel.com.pl/pl/cvd
https://www.aksel.com.pl/en/cvd
https://www.interloco.com.pl/cvd
https://conselplus.com/cvd

Zgłoszenie podatności powinno zawierać:

- opis problemu wraz z krokami pozwalającymi go odtworzyć,
- nazwę, wersję i środowisko dotkniętego produktu,
- materiały poglądowe — np. proof of concept, zrzuty ekranu, logi.

Zgłoszenia mogą być nadsyłane anonimowo. Trzeba jednak liczyć się z tym, że przy braku danych kontaktowych nie będziemy w stanie potwierdzić odbioru zgłoszenia ani przekazywać informacji o jego dalszym statusie.

Co dzieje się po zgłoszeniu

Etap	Co robimy
Potwierdzenie	Potwierdzamy otrzymanie zasadnego zgłoszenia w terminie wynikającym z unijnego rozporządzenia Cyber Resilience Act.
Analiza	Oceniamy zgłoszenie pod kątem skali, wpływu i faktycznego zagrożenia.
Naprawa	Właściwy zespół techniczny przygotowuje i testuje poprawkę bądź działanie łagodzące.
Kontakt zwrotny	Informujemy zgłaszającego o postępach prac oraz, jeśli to zasadne, o planowanym terminie publicznego ujawnienia.
Zamknięcie	Po wdrożeniu poprawki dokumentujemy sprawę wewnętrznie, a w uzasadnionych przypadkach publikujemy informację o niej — z podaniem autora zgłoszenia, o ile wyraził na to zgodę.

Czego nie traktujemy jako podatności

- problemów spowodowanych błędną konfiguracją albo nieprawidłowym lub ryzykownym użyciem produktu przez użytkownika,
- zgłoszeń dotyczących komponentów firm trzecich, na które nie mamy wpływu,
- kwestii czysto teoretycznych lub o znikomym znaczeniu praktycznym,
- surowych wyników skanerów automatycznych bez opisu i możliwych do odtworzenia dowodów.

Nasze zobowiązanie wobec badaczy (safe harbor)

Cenimy uczciwą współpracę z osobami zajmującymi się bezpieczeństwem. Jeżeli zgłaszający działa zgodnie z niniejszą polityką i w dobrej wierze, Aksel Sp. z o.o. nie będzie podejmować wobec niego kroków prawnych w związku z wykryciem i zgłoszeniem podatności.
W zamian oczekujemy, że badacz dołoży starań, by w trakcie testów nie naruszyć prywatności osób trzecich, nie zakłócić działania usług i nie doprowadzić do utraty danych.

Aktualizacje dokumentu

Niniejsza polityka stanowi element szerszej Polityki Skoordynowanego Ujawniania Podatności (Coordinated Vulnerability Disclosure) Aksel Sp. z o.o. Przeglądamy ją co najmniej raz do roku, a także w razie istotnych zmian organizacyjnych lub prawnych.

Kontakt

Zespół ds. Cyberbezpieczeństwa — Aksel Sp. z o.o.
E-mail: cybersecurity@aksel.com.pl
Strona: aksel.com.pl/cvd