

Polityka ujawniania podatności

1. Zakres polityki

Polityka dotyczy sprzętu, oprogramowania i firmware dostarczanych pod marką DIGITEX, w tym sterowników i urządzeń systemów alarmowania oraz oprogramowania digitexWAVE. Obejmuje również podatności komponentów zewnętrznych, jeżeli wpływają na bezpieczeństwo produktu DIGITEX.

Zgłoszenia przyjmujemy od użytkowników, administratorów, integratorów, badaczy i zespołów reagowania. Można zgłosić podejrzenie podatności bez kompletnego dowodu. Przyjmujemy także informacje o starszych wersjach; dostępne środki naprawcze zależą od produktu i jego okresu wsparcia, z uwzględnieniem obowiązków prawnych.

2. Kontakt i bezpieczne przekazanie informacji

Zgłoszenia bezpieczeństwa: security@digitex.pl lub psirt@digitex.pl .

Aktualny kontakt i ta polityka: <https://www.digitex.pl/polityka-podatnosci/>

Obsługujemy zgłoszenia w języku polskim i angielskim. Kanał przyjmuje zgłoszenia przez całą dobę. Odpowiedź zawiera identyfikator sprawy oraz następny krok lub prośbę o dodatkowe informacje. Automatyczne potwierdzenie wpływu nie stanowi odpowiedzi.

Zgłoszenia wskazujące na trwający atak albo możliwość nieuprawnionego uruchomienia lub zablokowania alarmowania wymagają pilnej oceny bez zbędnego oczekiwania.

W pierwszej wiadomości nie przysyłaj hasel, kluczy, danych osobowych mieszkańców ani pełnych kopii systemów. Jeżeli dowody zawierają informacje wrażliwe, poproś o uzgodnienie bezpiecznego sposobu przekazania. Nie zakładaj, że zwykły e-mail zapewnia szyfrowanie od nadawcy do odbiorcy.

3. Jak przygotować zgłoszenie

W temacie wiadomości wpisz „Podatność bezpieczeństwa – nazwa produktu”. Jeżeli podejrzewasz trwający atak lub zagrożenie dla alarmowania, dodaj „PILNE”. Przekaż tyle informacji, ile możesz bezpiecznie udostępnić:

- Nazwa i model produktu, wersja oprogramowania lub firmware oraz sposób jej ustalenia; identyfikator urządzenia, jeżeli jest potrzebny do analizy.
- Opis problemu, data i czas jego zaobserwowania ze strefą czasową oraz warunki wystąpienia.
- Możliwy skutek, np. dostęp bez uprawnień, zmiana ustawień, utrata łączności lub nieprawidłowe wykonanie komendy.
- Informacja, czy problem został zaobserwowany w działającym systemie, czy w laboratorium; ewentualne przesłanki aktywnego wykorzystania i wcześniejszej publikacji.

- Bezpieczny opis odtworzenia, zanonimizowany fragment logu lub zrzut ekranu. Nie odtwarzaj błędów na działających syrenach tylko po to, aby przygotować dowód.
- Kontakt do odpowiedzi oraz preferencja dotycząca podania autorstwa przy publikacji. Zgłoszenie anonimowe też przyjmujemy, ale bez kanału zwrotnego nie prześlemy potwierdzenia ani pytań.

4. Zasady bezpiecznego badania

Badania prowadź na własnym środowisku testowym albo za wyraźną zgodą uprawnionego właściciela systemu, w uzgodnionym zakresie. Ta polityka nie jest upoważnieniem do testowania instalacji klientów ani infrastruktury osób trzecich.

Nie uruchamiaj syren, komunikatów głosowych ani innych wyjść wykonawczych w systemie produkcyjnym. Nie blokuj możliwości nadania rzeczywistego alarmu.

Nie prowadź testów przeciążeniowych, łamania haseł, socjotechniki ani działań niszczących dane bez odrębnie uzgodnionego upoważnienia i planu bezpieczeństwa.

Ogranicz dostęp do danych do niezbędnego minimum. Jeżeli uzyskasz dostęp do cudzych danych, przerwij badanie, nie kopiuj kolejnych danych i poinformuj o tym w zgłoszeniu.

Po uzyskaniu wystarczającej informacji o luce zakończ próbę. Nie rozszerzaj dostępu i nie utrzymuj go po zakończeniu badania.

Zależy nam na współpracy w dobrej wierze. Nie wymagamy podpisania umowy o poufności jako warunku przyjęcia zgłoszenia. Polityka nie ustanawia programu nagród ani gwarancji wynagrodzenia; ewentualne odrębne ustalenia wymagają uzgodnienia z DIGITEX.

5. Jak obsługujemy zgłoszenie

Po rejestracji ustalamy, którego produktu i wersji dotyczy sprawa, czy można odtworzyć problem i jakie mogą być jego skutki. Możemy poprosić o dodatkowe informacje. Gdy zgłoszenie jest duplikatem albo nie potwierdzimy podatności, wyjaśniamy wynik oceny.

Priorytet zależy od ryzyka dla użytkowników. Szczególną wagę mają: możliwość nieuprawnionego alarmowania, zablokowania ostrzegania, przejęcia administracji, wykorzystania luki bez uwierzytelnienia oraz dowody rzeczywistego ataku. Ocena techniczna, np. CVSS, jest informacją pomocniczą i nie zastępuje oceny skutków dla instalacji.

Dobieramy i sprawdzamy poprawkę lub środek ograniczający ryzyko. Ze zgłaszającym uzgadniamy termin kolejnej informacji; jeżeli rozwiązanie potrwa dłużej, przekazujemy status i przyczynę. Nie wyznaczamy jednego terminu naprawy dla wszystkich przypadków. Zmiany muszą uwzględniać ciągłość i poprawność alarmowania.

6. Poufność i skoordynowana publikacja

Informacje ze zgłoszenia udostępniamy osobom niezbędnym do analizy i usunięcia problemu. W uzasadnionych przypadkach współpracujemy z integratorem, dostawcą komponentu lub

właściwym zespołem CSIRT. Dane przekazujemy w zakresie potrzebnym do obsługi sprawy i realizacji obowiązków prawnych.

Prosimy o uzgodnienie terminu publikacji szczegółów technicznych tak, aby użytkownicy mogli zastosować zabezpieczenia. Nie wstrzymujemy koniecznego ostrzeżenia użytkowników ani obowiązkowego raportowania tylko dlatego, że nie zakończono prac nad poprawką. W razie rozbieżności możemy skorzystać z pomocy koordynatora, np. CERT Polska.

Komunikat bezpieczeństwa wskazuje produkty i wersje objęte problemem, jego skutki, zalecane działania, dostępność poprawki oraz ograniczenia rozwiązania tymczasowego. Dane autora zgłoszenia publikujemy wyłącznie po uzyskaniu jego zgody. Miejsce publikacji komunikatów: www.digitex.pl

Dane kontaktowe i materiały ze zgłoszenia przetwarzamy zgodnie z informacją o prywatności dostępną pod adresem www.digitex.pl.

7. Zgłoszenie do DIGITEX a raportowanie CRA

Zgłoszenie podatności do DIGITEX uruchamia jej ocenę. Jeżeli uzyskane informacje wskazują na aktywnie wykorzystywaną podatność lub poważny incydent dotyczący bezpieczeństwa produktu objętego CRA, realizujemy obowiązki raportowania do właściwych organów. Termin pierwszej odpowiedzi zgłaszającemu nie zastępuje tych obowiązków. Użytkownicy otrzymują bez zbędnej zwłoki informacje potrzebne do ograniczenia skutków zdarzenia, stosownie do obowiązujących wymagań.

Awarię wymagającą natychmiastowej interwencji serwisowej zgłoś również kanałem określonym w umowie utrzymaniowej. Skrzynka podatności nie zastępuje dyżuru operacyjnego ani numerów alarmowych.