Polityka ujawniania luk w zabezpieczeniach

Certum

16 października 2026

Wprowadzenie

Certum jest zaangażowane w zapewnienie bezpieczeństwa klientów poprzez ochronę ich danych. Niniejsza polityka ma na celu dostarczenie analitykom bezpieczeństwa jasnych wytycznych dotyczących prowadzenia działań związanych z wykrywaniem luk w zabezpieczeniach oraz przedstawienie naszych preferencji dotyczących sposobu zgłaszania nam wykrytych luk.

Niniejsza polityka opisuje, jakie systemy i rodzaje analiz bezpieczeństwa są nią objęte, w jaki sposób należy przesyłać nam zgłoszenia dotyczące luk w zabezpieczeniach oraz jak długo prosimy analityków zajmujących się bezpieczeństwem o wstrzymanie się z publicznym ujawnieniem luk.

Zachęcamy do kontaktowania się z nami w celu zgłaszania potencjalnych luk w zabezpieczeniach naszych systemów.

Upoważnienie

Jeśli podczas prowadzenia badań i analiz nad bezpieczeństwem dołożysz starań w dobrej wierze, aby przestrzegać niniejszych wytycznych, uznamy Twoje badania za autoryzowane, będziemy współpracować z Tobą w celu szybkiego zrozumienia i rozwiązania problemu, a Certum nie będzie zalecać ani podejmować działań prawnych związanych z Twoimi badaniami. W przypadku wszczęcia przez stronę trzecią postępowania prawnego przeciwko Tobie w związku z działaniami przeprowadzonymi zgodnie z niniejszymi wytycznymi, poinformujemy o tej autoryzacji.

Wytyczne

W ramach niniejszej polityki termin „badania, Analiza” oznacza działania, w ramach których:

- Powiadom nas jak najszybciej po wykryciu rzeczywistego lub potencjalnego problemu bezpieczeństwa.
- Dokładają Państwo wszelkich starań, aby uniknąć naruszenia prywatności, pogorszenia komfortu użytkowania, zakłóceń w działaniu systemów produkcyjnych oraz zniszczenia lub manipulacji danymi.
- Wykorzystujesz luki w zabezpieczeniach wyłącznie w zakresie niezbędnym do potwierdzenia istnienia luki. Nie wykorzystujesz luki w celu naruszenia bezpieczeństwa lub wykradzenia danych, uzyskania stałego dostępu do wiersza poleceń ani przejścia do innych systemów.
- Należy zapewnić nam określony (racjonalny) czas na rozwiązanie problemu przed jego publicznym ujawnieniem.
- Nie należy przesyłać dużej liczby zgłoszeń o niskiej jakości.

Po stwierdzeniu istnienia luki w zabezpieczeniach lub napotkaniu jakichkolwiek danych wrażliwych (w tym danych osobowych, informacji finansowych, informacji zastrzeżonych lub tajemnic handlowych jakiejkolwiek strony) należy przerwać test, niezwłocznie nas o tym powiadomić i nie ujawniać tych danych nikomu innemu.

Metody testowania

Następujące metody testowania są niedozwolone:

- Testy typu „odmowa usługi” (DoS lub DDoS) lub inne testy, które utrudniają dostęp do systemu lub danych albo powodują ich uszkodzenie
- Testy fizyczne (np. dostęp do biura, otwarte drzwi, itp.), socjotechnika (np. phishing, vishing) lub wszelkie inne nietechniczne testy podatności

Zakres

Niniejsza polityka ma zastosowanie do następujących systemów i usług:

- SimplySign SAM (Signature Activation Module),
- SmartSign,
- SimplySign Desktop,
- Aplikacje mobilne SimplySign(Android, IOS).

Wszelkie usługi, które nie zostały wyraźnie wymienione powyżej, takie jak usługi powiązane, są wyłączone z zakresu niniejszej polityki i nie są dopuszczone do testowania. Ponadto luki w zabezpieczeniach wykryte w systemach naszych dostawców wykraczają poza zakres niniejszej polityki i należy je zgłaszać bezpośrednio do dostawcy zgodnie z jego polityką ujawniania informacji (jeśli taka istnieje). Jeśli nie masz pewności, czy dany system znajduje się w zakresie niniejszej polityki, skontaktuj się z nami pod https://www.certum.pl/pl/bezpieczenstwo-podatnosci-kontakt/, przed rozpoczęciem badań.

Prosimy, aby aktywne badania, analizy i testy były prowadzone wyłącznie na systemach i usługach objętych zakresem niniejszego dokumentu. Jeśli istnieje konkretny system spoza zakresu, który Twoim zdaniem zasługuje na przetestowanie, skontaktuj się z nami, aby najpierw to omówić. Z czasem będziemy rozszerzać zakres niniejszej polityki.

Zgłaszanie luk w zabezpieczeniach

Informacje przekazane zgodnie z niniejszą polityką będą wykorzystywane wyłącznie w celach obronnych – w celu ograniczenia lub usunięcia luk w zabezpieczeniach. Jeśli Państwa ustalenia obejmują nowo odkryte luki w zabezpieczeniach, które mają wpływ na wszystkich użytkowników produktu lub usługi, a nie wyłącznie na ADS, możemy udostępnić Państwa zgłoszenie Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), gdzie zostanie ono rozpatrzone w ramach koordynowanego przez ten zespół procesu ujawniania luk w zabezpieczeniach. Nie udostępnimy Państwa imienia i nazwiska ani danych kontaktowych bez wyraźnej zgody.

Zgłoszenia luk w zabezpieczeniach przyjmujemy za pośrednictwem strony internetowej lub formularza znajdującego się na stronie: https://www.certum.pl/pl/bezpieczenstwo-podatnosci-kontakt/ Zgłoszenia można przesyłać anonimowo. Jeśli podasz dane kontaktowe, potwierdzimy otrzymanie zgłoszenia w ciągu 3 dni roboczych.

Czego oczekujemy od Państwa

Aby pomóc nam w klasyfikacji i ustalaniu priorytetów zgłoszeń, zalecamy, aby Państwa zgłoszenia:

- Opisywały miejsce wykrycia luki oraz potencjalne skutki jej wykorzystania.
- Zawierały szczegółowy opis kroków niezbędnych do odtworzenia luki (pomocne są skrypty potwierdzające koncepcję lub zrzuty ekranu).

- Były sporządzone w języku polskim i/lub angielskim, jeśli to możliwe.

Czego możesz oczekiwać od nas

Jeśli zdecydujesz się udostępnić nam swoje dane kontaktowe, zobowiązujemy się do jak najszybszej i jak najbardziej otwartej współpracy z Tobą.

- W ciągu 3 dni roboczych potwierdzimy otrzymanie zgłoszenia.
- W miarę naszych możliwości potwierdzimy istnienie luki i zapewnimy jak największą przejrzystość co do działań podejmowanych w trakcie procesu naprawy, w tym w odniesieniu do problemów lub wyzwań, które mogą opóźnić rozwiązanie.
- Będziemy prowadzić otwarty dialog w celu omówienia problemów.

Pytania

Pytania dotyczące niniejszej polityki można kierować na adres infolinia@certum.pl. Zapraszamy również do kontaktowania się z nami w sprawie sugestii dotyczących ulepszenia niniejszej polityki.

Historia zmian dokumentu

Wersja	Data	Opis
1.0	16.10.2026 r.	Inicjalna wersja polityki.