# POLITYKA UJAWNIANIA PODATNOŚCI (CVD)

| Dotyczy / Norma | Opracował: | Zatwierdził: |
|---|---|---|
| **CRA (Cyber Resilience Act) Rozporządzenie (UE) 2024/2847** | **GFLEAN Pełnomocnik ds. cyberbezpieczeństwa** | **Prezes Zarządu BRAGER Sp. z o.o. Rafał Urbaniak** |

## Karta dokumentu

| Pole | Wartość |
|---|---|
| Nazwa dokumentu | Polityka skoordynowanego ujawniania podatności (CVD) |
| Numer dokumentu | PA-CVD-01 |
| Wydanie / wersja | Wydanie 2 / wersja 2.0 |
| Data wydania | 30.06.2026 |
| Data wejścia w życie | 30.06.2026 |
| Właściciel dokumentu | Pełnomocnik ds. cyberbezpieczeństwa / właściciel procesu bezpieczeństwa produktu |
| Zatwierdza | Prezes Zarządu BRAGER Sp. z o.o. |
| Przegląd okresowy | Nie rzadziej niż raz w roku oraz po istotnym incydencie, zmianie produktu lub zmianie wymagań prawnych |
| Status | Dokument do stosowania w systemie zgodności CRA |

## Karta zmian

| Wydanie | Data | Opis zmiany | Opracował | Zatwierdził |
|---|---|---|---|---|
| 1 | 24.03.2026 | Pierwsze opracowanie polityki ujawniania podatności. | GFLEAN | Prezes Zarządu |
| 2 | 30.06.2026 | Aktualizacja struktury dokumentu, doprecyzowanie kanałów zgłoszeń, klasyfikacji podatności, terminów obsługi, raportowania CRA, rejestrów i powiązań z Polityką bezpieczeństwa produktu wg CRA. | GFLEAN | Prezes Zarządu |

## 1. Cel

Celem niniejszej Polityki skoordynowanego ujawniania podatności (CVD) jest ustanowienie zasad przyjmowania, oceny, obsługi, usuwania i kontrolowanego ujawniania informacji o podatnościach dotyczących produktów z elementami cyfrowymi oferowanych, rozwijanych lub utrzymywanych przez BRAGER Sp. z o.o., zgodnie z wymaganiami Cyber Resilience Act (CRA).

Polityka określa jednolity sposób postępowania z informacjami o podatnościach pochodzącymi ze źródeł wewnętrznych i zewnętrznych, tak aby ograniczać ryzyko dla użytkowników, zapewniać transparentną komunikację i utrzymywać zgodność produktów w całym okresie wsparcia.

**Polityka ma w szczególności zapewnić:**

- bezpieczny i przejrzysty kanał zgłaszania podatności przez badaczy bezpieczeństwa, klientów, partnerów, dostawców oraz użytkowników końcowych,
- terminową analizę, klasyfikację i ograniczanie ryzyka wynikającego z podatności,
- skoordynowane ujawnianie informacji o podatnościach w sposób ograniczający ryzyko nadużyć,
- udokumentowanie działań wymaganych przez CRA w zakresie obsługi podatności przez cały okres wsparcia produktu,
- powiązanie procesu CVD z aktualizacjami bezpieczeństwa, obsługą incydentów, rejestrem podatności i oceną ryzyka produktu.

## 2. Zakres stosowania

Polityka obejmuje produkty z elementami cyfrowymi projektowane, rozwijane, wytwarzane, wprowadzane do obrotu lub utrzymywane przez BRAGER Sp. z o.o., w szczególności:

- sterowniki kotłów i instalacji grzewczych, w tym sterowniki lokalne oraz sterowniki z funkcjami komunikacyjnymi,
- moduły komunikacyjne, w tym rozwiązania Internet/GSM oraz urządzenia umożliwiające zdalny dostęp,
- firmware, oprogramowanie wbudowane, aplikacje, interfejsy użytkownika, panele HMI i porty serwisowe,
- powiązane usługi zdalnego przetwarzania danych, jeżeli są niezbędne do realizacji funkcji produktu,
- komponenty programowe lub sprzętowe dostarczane oddzielnie, o ile pozostają w zakresie odpowiedzialności BRAGER Sp. z o.o.

Polityka ma zastosowanie do pracowników, współpracowników, dostawców i podwykonawców zaangażowanych w rozwój, utrzymanie i serwis produktów, a także do osób trzecich zgłaszających podatności.

Polityka nie obejmuje zgłoszeń niezwiązanych z bezpieczeństwem produktu, reklamacji handlowych, usterek użytkowych bez wpływu na cyberbezpieczeństwo oraz incydentów dotyczących systemów osób trzecich pozostających poza kontrolą BRAGER Sp. z o.o., chyba że wpływają one na bezpieczeństwo produktu objętego zakresem CRA.

## 3. Podstawa prawna i normatywna

Niniejsza Polityka realizuje obowiązki producenta wynikające z Cyber Resilience Act, w szczególności w zakresie ustanowienia procesów obsługi podatności, wdrożenia polityki coordinated vulnerability disclosure, dostarczania środków naprawczych oraz raportowania aktywnie wykorzystywanych podatności i poważnych incydentów.

Dokument wspiera również podejście zgodne z dobrymi praktykami norm i standardów bezpieczeństwa, w szczególności ISO/IEC 29147 (ujawnianie podatności), ISO/IEC 30111 (obsługa podatności), ISO/IEC 27001 (zarządzanie bezpieczeństwem informacji) oraz IEC 62443 (cyberbezpieczeństwo systemów automatyki i sterowania).

| Obszar | Wymaganie / oczekiwany rezultat |
|---|---|
| CRA - podatności | Producent posiada proces przyjmowania, analizy, usuwania i dokumentowania podatności przez okres wsparcia produktu. |
| CRA - CVD | Producent zapewnia publicznie dostępny i użyteczny kanał zgłaszania podatności oraz zasady skoordynowanego ujawniania informacji. |
| CRA - raportowanie | Aktywnie wykorzystywane podatności i poważne incydenty są eskalowane i raportowane zgodnie z wymaganiami CRA. |
| Dokumentacja techniczna | Działania dotyczące podatności są rejestrowane i stanowią część dowodów zgodności produktu. |

## 4. Definicje

| Pojęcie | Definicja stosowana w BRAGER Sp. z o.o. |
|---|---|
| Podatność | Słabość, błąd, luka, niewłaściwa konfiguracja lub brak zabezpieczenia, które mogą zostać wykorzystane do naruszenia poufności, integralności, dostępności, autentyczności lub bezpieczeństwa produktu. |
| Zgłaszający | Osoba fizyczna lub prawna przekazująca informację o potencjalnej podatności. |
| CVD | Skoordynowane ujawnienie podatności, czyli proces przyjęcia, analizy, usunięcia i kontrolowanego ujawnienia informacji o podatności w sposób ograniczający ryzyko dla użytkowników. |
| Aktywnie wykorzystywana podatność | Podatność, co do której istnieją wiarygodne przesłanki, że jest wykorzystywana w praktyce lub istnieje potwierdzony scenariusz jej aktywnej eksploatacji. |
| Poważny incydent | Incydent mający wpływ na bezpieczeństwo produktu z elementami cyfrowymi w rozumieniu CRA. |
| Środek naprawczy | Aktualizacja bezpieczeństwa, poprawka, zmiana konfiguracji, obejście tymczasowe, wyłączenie funkcji lub komunikat bezpieczeństwa ograniczający ryzyko. |
| Okres wsparcia | Okres, w którym BRAGER Sp. z o.o. zapewnia utrzymanie bezpieczeństwa produktu, w tym obsługę podatności i dostarczanie aktualizacji bezpieczeństwa. |

## 5. Zasady ogólne

- BRAGER Sp. z o.o. wspiera odpowiedzialne, legalne i działające w dobrej wierze zgłaszanie podatności.
- Każde zgłoszenie jest traktowane poufnie i analizowane z należytą starannością.
- Informacje o podatnościach są ujawniane publicznie dopiero po wdrożeniu środka naprawczego lub ograniczającego ryzyko, chyba że wcześniejsze ujawnienie jest niezbędne dla ochrony użytkowników.
- Producent nie podejmuje działań odwetowych wobec zgłaszających, którzy działają legalnie, w dobrej wierze i zgodnie z niniejszą Polityką.
- Obsługa podatności jest prowadzona z uwzględnieniem wpływu na bezpieczeństwo użytkowników, integralność produktów oraz obowiązki raportowe CRA.
- Wszystkie działania dotyczące podatności muszą być dokumentowane w rejestrze zgłoszeń podatności.

## 6. Zasady bezpiecznego testowania przez zgłaszających

Zgłaszający działający w dobrej wierze powinien ograniczyć swoje działania do niezbędnego minimum pozwalającego potwierdzić podatność. Niedopuszczalne są działania, które mogą naruszać dostępność usług, bezpieczeństwo użytkowników lub przepisy prawa.

**Zgłaszający powinien unikać w szczególności:**

- ataków typu DoS/DDoS, testów obciążeniowych i działań zakłócających dostępność produktu lub usługi,
- uzyskiwania, kopiowania, modyfikowania lub usuwania danych innych użytkowników,
- wykorzystywania podatności poza zakresem niezbędnym do jej potwierdzenia,
- socjotechniki, phishingu, prób uzyskania dostępu do pracowników lub dostawców,
- testów fizycznych na urządzeniach niebędących własnością zgłaszającego lub bez zgody właściciela,
- publikowania szczegółów technicznych podatności przed zakończeniem procesu CVD lub bez uzgodnienia z BRAGER Sp. z o.o.

# 7. Kanały zgłaszania podatności

Zgłoszenia podatności należy kierować na dedykowany adres e-mail: **security@brager.com.pl**. Jeżeli BRAGER Sp. z o.o. udostępni formularz zgłoszeniowy, portal lub system ticketowy, kanał ten może być stosowany jako kanał równoległy lub podstawowy, zgodnie z informacją opublikowaną na stronie producenta.

Zgłoszenie powinno zawierać, w miarę możliwości:

- nazwę produktu, model, wersję sprzętową i wersję firmware/oprogramowania,
- opis podatności oraz warunki jej wystąpienia,
- kroki odtworzenia podatności,
- ocenę potencjalnego wpływu na poufność, integralność, dostępność, autentyczność lub bezpieczeństwo produktu,
- dowody techniczne, np. logi, zrzuty ekranu, konfigurację testową, proof of concept,
- informację, czy podatność może być aktywnie wykorzystywana,
- dane kontaktowe zgłaszającego oraz preferowany sposób komunikacji.

BRAGER Sp. z o.o. dopuszcza zgłoszenia anonimowe, jednak brak danych kontaktowych może utrudnić analizę, potwierdzenie i koordynację ujawnienia podatności.

# 8. Obsługa zgłoszeń

Proces obsługi zgłoszenia podatności obejmuje poniższe etapy:

| Etap | Opis działania | Termin operacyjny |
|---|---|---|
| 1. Przyjęcie | Rejestracja zgłoszenia w rejestrze podatności i nadanie numeru sprawy. | Niezwłocznie po otrzymaniu |
| 2. Potwierdzenie | Potwierdzenie otrzymania zgłoszenia zgłaszającemu, o ile przekazał dane kontaktowe. | Do 3 dni roboczych |
| 3. Wstępna kwalifikacja | Sprawdzenie, czy zgłoszenie dotyczy produktu BRAGER, czy ma charakter bezpieczeństwa i czy jest kompletne. | Do 5 dni roboczych |
| 4. Analiza techniczna | Odtworzenie podatności, ocena wpływu, ustalenie priorytetu i określenie ryzyka. | Zależnie od poziomu ryzyka |
| 5. Decyzja | Określenie sposobu postępowania: poprawka, obejście, komunikat, koordynacja z dostawcą lub zamknięcie jako niepotwierdzone. | Po zakończeniu analizy |
| 6. Działanie naprawcze | Opracowanie, test i wdrożenie środka naprawczego lub ograniczającego ryzyko. | Bez zbędnej zwłoki |
| 7. Komunikacja | Poinformowanie zgłaszającego i użytkowników, jeżeli jest to wymagane. | Zależnie od wpływu i ryzyka |
| 8. Zamknięcie | Udokumentowanie decyzji, działań, dat i ewentualnego raportowania do organów. | Po wdrożeniu i weryfikacji działań |

# 9. Klasyfikacja i priorytetyzacja podatności

Podatności są klasyfikowane co najmniej według wpływu na poufność, integralność, dostępność, autentyczność i bezpieczeństwo produktu, łatwości wykorzystania, zakresu narażenia użytkowników, dostępności obejść oraz informacji o rzeczywistym wykorzystaniu. BRAGER Sp. z o.o. może stosować metody oceny takie jak CVSS, jednak wynik punktowy nie zastępuje oceny ryzyka produktowego i kontekstu bezpieczeństwa instalacji.

| Priorytet | Kryteria przykładowe | Minimalne działanie |
|---|---|---|
| Krytyczny | Aktywne wykorzystanie; możliwość zdalnego przejęcia kontroli; bezpośredni wpływ na bezpieczeństwo pracy instalacji; brak obejścia. | Natychmiastowa eskalacja, analiza awaryjna, decyzja raportowa CRA, pilny środek naprawczy lub ograniczający ryzyko. |
| Wysoki | Znaczący wpływ na integralność, dostępność lub bezpieczeństwo produktu; możliwa eksploatacja zdalna lub szeroka skala narażenia. | Priorytetowe opracowanie poprawki, komunikacja z użytkownikami i |

| | | |
|---|---|---|
| | | monitorowanie wykorzystania. |
| Średni | Ograniczony wpływ, wymagane szczególne warunki wykorzystania lub dostęp lokalny; istnieją środki ograniczające ryzyko. | Zaplanowanie poprawki, obejście tymczasowe lub zmiana konfiguracji. |
| Niski | Niewielki wpływ na bezpieczeństwo lub mało prawdopodobny scenariusz wykorzystania. | Rejestracja, monitorowanie i uwzględnienie w planie utrzymania produktu. |

## 10. Działania naprawcze i ograniczające ryzyko

Dla potwierdzonych podatności BRAGER Sp. z o.o. wdraża odpowiedni środek naprawczy lub ograniczający ryzyko adekwatny do poziomu ryzyka, możliwości technicznych produktu oraz obowiązków CRA. Działania naprawcze muszą zostać przetestowane, udokumentowane i przekazane użytkownikom w sposób możliwy do zastosowania.

Środkami naprawczymi lub ograniczającymi ryzyko mogą być w szczególności:

- aktualizacja bezpieczeństwa firmware lub oprogramowania,
- zmiana konfiguracji lub zmiana ustawień domyślnych,
- obejście tymczasowe ograniczające możliwość wykorzystania podatności,
- wyłączenie podatnej funkcji lub ograniczenie dostępu do niej,
- komunikat bezpieczeństwa dla użytkowników, instalatorów i serwisu,
- działania koordynacyjne z dostawcą komponentu, jeżeli podatność dotyczy elementu zewnętrznego.

W przypadku podatności dotyczącej komponentu dostawcy lub strony trzeciej BRAGER Sp. z o.o. podejmuje działania koordynacyjne z odpowiednim podmiotem, zachowując poufność oraz wymagania CRA dotyczące bezpieczeństwa produktu.

## 11. Komunikacja ze zgłaszającym

BRAGER Sp. z o.o. utrzymuje kontakt ze zgłaszającym w zakresie niezbędnym do doprecyzowania zgłoszenia, uzgodnienia terminu publikacji oraz potwierdzenia wdrożenia środka naprawczego. Zakres przekazywanych informacji zależy od statusu sprawy, ryzyka nadużyć i wymogów poufności.

Co do zasady zgłaszający otrzymuje informacje o:

- przyjęciu zgłoszenia,
- wyniku wstępnej kwalifikacji,
- potwierdzeniu lub braku potwierdzenia podatności,
- planowanym sposobie postępowania, jeżeli może zostać ujawniony bez zwiększenia ryzyka,
- orientacyjnym terminie publicznego ujawnienia, jeżeli jest planowane,
- zamknięciu sprawy.

BRAGER Sp. z o.o. może publicznie podziękować zgłaszającemu, o ile zgłaszający wyrazi na to zgodę.

## 12. Publiczne ujawnienie informacji

Informacja o potwierdzonej podatności może zostać opublikowana po wydaniu poprawki, wdrożeniu środka tymczasowego lub poinformowaniu użytkowników o ryzyku i sposobie ograniczenia skutków. Publikacja powinna być skoordynowana z działaniami naprawczymi i nie może nieuzasadnienie zwiększać ryzyka wykorzystania podatności.

Komunikat o podatności powinien zawierać co najmniej:

- identyfikację produktu, modelu i wersji,
- opis podatności w zakresie bezpiecznym do ujawnienia,
- ocenę wpływu i poziom ryzyka,
- informację o dostępnej aktualizacji, obejściu lub innym środku ograniczającym ryzyko,
- zalecenia dla użytkowników, instalatorów i serwisu,
- datę publikacji oraz dane kontaktowe do zgłoszeń uzupełniających.

BRAGER Sp. z o.o. może opóźnić publikację szczegółów technicznych, jeżeli ich ujawnienie zwiększałoby ryzyko nadużyć przed wdrożeniem środków ochronnych.

## 13. Raportowanie do właściwych organów zgodnie z CRA

Jeżeli BRAGER Sp. z o.o. uzyska wiedzę o aktywnie wykorzystywanej podatności dotyczącej produktu objętego CRA lub o poważnym incydencie mającym wpływ na bezpieczeństwo takiego produktu, uruchamia obowiązkowy tryb eskalacji i raportowania zgodnie z wymaganiami CRA.

| Krok | Działanie wewnętrzne | Termin operacyjny |
|---|---|---|
| 1 | Eskalacja do właściciela procesu bezpieczeństwa produktu / Pełnomocnika ds. cyberbezpieczeństwa. | Niezwłocznie, nie później niż 4 godziny od potwierdzenia przesłanek |
| 2 | Ocena, czy zdarzenie spełnia przesłanki raportowania CRA. | Nie później niż 12 godzin od eskalacji |
| 3 | Przygotowanie danych do zgłoszenia oraz decyzja o zakresie informacji. | Bez zbędnej zwłoki |
| 4 | Złożenie wymaganego zgłoszenia przez właściwy kanał raportowy. | Zgodnie z terminami CRA |
| 5 | Prowadzenie dokumentacji, raportów uzupełniających i raportu końcowego. | Do zamknięcia sprawy |

Za przygotowanie zgłoszenia odpowiada właściciel procesu bezpieczeństwa produktu przy współpracy zespołu technicznego, działu prawnego/compliance oraz Zarządu. Rejestr zgłoszeń do organów jest prowadzony jako część dokumentacji zgodności CRA.

## 14. Role i odpowiedzialności

| Rola / funkcja | Odpowiedzialność |
|---|---|
| Zarząd | Zatwierdza Politykę, zapewnia zasoby, podejmuje decyzje strategiczne i akceptuje istotne ryzyka oraz komunikację zewnętrzną w sprawach krytycznych. |
| Pełnomocnik ds. cyberbezpieczeństwa / właściciel procesu | Nadzoruje realizację Polityki, koordynuje zgłoszenia, klasyfikację, komunikację, rejestry i raportowanie CRA. |
| Zespół techniczny / R&D / produktowy | Analizuje podatności, odtwarza scenariusze, przygotowuje poprawki, obejścia i testy bezpieczeństwa. |
| IT / administrator usług zdalnych | Wspiera analizę zdarzeń dotyczących infrastruktury zdalnej, logów, usług komunikacyjnych i dostępności. |
| Dział prawny / compliance | Ocena obowiązków regulacyjnych, ryzyk prawnych, zasad poufności oraz treści komunikatów publicznych. |
| Obsługa klienta / support / serwis | Przyjmuje sygnały od klientów, dystrybuuje zalecenia, wspiera użytkowników w zastosowaniu poprawek i obejść. |
| Dostawcy i podwykonawcy | Współpracują w zakresie podatności komponentów, poprawek i informacji technicznych zgodnie z umowami i wymaganiami bezpieczeństwa. |

## 15. Dokumentowanie i rejestry

BRAGER Sp. z o.o. prowadzi rejestr zgłoszeń podatności. Rejestr stanowi element dokumentacji zgodności CRA oraz podstawę do oceny skuteczności procesu CVD.

Rejestr obejmuje co najmniej:

- numer sprawy i datę wpływu zgłoszenia,
- źródło zgłoszenia i dane kontaktowe zgłaszającego, jeżeli zostały przekazane,
- produkt, model, wersję sprzętową i wersję firmware/oprogramowania,
- opis podatności i status weryfikacji,
- ocenę ryzyka, priorytet i decyzje klasyfikacyjne,
- przypisane osoby odpowiedzialne,
- działania naprawcze, testy i daty wdrożenia,
- daty komunikacji ze zgłaszającym i użytkownikami,
- informację o ewentualnym zgłoszeniu do CSIRT/ENISA lub właściwych organów,
- datę zamknięcia sprawy i wnioski doskonalące.

Dokumentacja jest przechowywana przez okres wynikający z wymagań CRA, polityki retencji dokumentacji technicznej oraz wymagań umownych, nie krócej niż przez okres utrzymywania dokumentacji zgodności produktu.

## 16. Poufność i ochrona informacji

- Informacje o nieujawnionych podatnościach są traktowane jako poufne.
- Dostęp do informacji o podatnościach mają wyłącznie osoby uprawnione i zaangażowane w obsługę sprawy.

- Publikacja szczegółów technicznych przed wdrożeniem środków naprawczych wymaga akceptacji właściciela procesu i, dla spraw wysokiego ryzyka, Zarządu.
- Dane osobowe przetwarzane w związku ze zgłoszeniami są obsługiwane zgodnie z właściwymi przepisami o ochronie danych i wewnętrznymi zasadami BRAGER Sp. z o.o.
- Wymiana informacji z dostawcami, podwykonawcami i organami odbywa się w zakresie niezbędnym do obsługi sprawy oraz zgodnie z zasadą minimalizacji informacji.

## 17. Relacja do innych dokumentów

Niniejsza Polityka jest dokumentem wykonawczym względem Polityki bezpieczeństwa produktów z elementami cyfrowymi wg CRA i jest powiązana z następującymi dokumentami:

- Polityka bezpieczeństwa produktów z elementami cyfrowymi wg CRA,
- Procedura zarządzania incydentami cyberbezpieczeństwa,
- Procedura zarządzania aktualizacjami bezpieczeństwa i firmware,
- Procedura oceny ryzyka produktu,
- Rejestr produktów objętych CRA,
- Rejestr podatności i rejestr incydentów,
- Plan minimalizacji ryzyk cyberbezpieczeństwa,
- Polityka retencji dokumentacji technicznej,
- Umowy i wymagania bezpieczeństwa dla dostawców oraz podwykonawców.

## 18. Monitoring skuteczności i przegląd

Skuteczność procesu CVD jest monitorowana przez właściciela procesu bezpieczeństwa produktu. Wyniki przeglądu są przekazywane Zarządowi lub osobie wyznaczonej do nadzoru nad zgodnością CRA.

| Wskaźnik | Opis |
|---|---|
| Liczba zgłoszeń podatności | Liczba zgłoszeń otrzymanych w okresie sprawozdawczym, z podziałem na potwierdzone, niepotwierdzone i poza zakresem. |
| Czas potwierdzenia zgłoszenia | Średni czas od wpływu zgłoszenia do potwierdzenia przyjęcia. |
| Czas kwalifikacji | Średni czas od wpływu zgłoszenia do wstępnej kwalifikacji. |
| Czas wdrożenia środka naprawczego | Czas od potwierdzenia podatności do udostępnienia poprawki lub obejścia. |
| Liczba podatności aktywnie wykorzystywanych | Liczba spraw wymagających eskalacji i oceny obowiązku raportowego CRA. |
| Liczba działań doskonalących | Liczba zmian w produkcie, procesie, dokumentacji lub dostawcach wynikających z obsługi podatności. |

Polityka podlega przeglądowi nie rzadziej niż raz w roku oraz po każdym istotnym incydencie, zmianie organizacyjnej, zmianie portfolio produktów lub zmianie wymogów prawnych.

## 19. Postanowienia końcowe

- Wszelkie odstępstwa od niniejszej Polityki wymagają udokumentowania i akceptacji właściciela procesu oraz, w sprawach istotnych, Zarządu.
- Polityka jest udostępniana wewnętrznie pracownikom i współpracownikom zaangażowanym w rozwój, produkcję, serwis i utrzymanie produktów.
- Zakres zewnętrzny Polityki, obejmujący zasady zgłaszania podatności i safe harbour, powinien być publicznie dostępny dla badaczy bezpieczeństwa, klientów i partnerów.
- Niniejsze wydanie zastępuje wcześniejsze wersje Polityki ujawniania podatności.

# Załącznik nr 1. Formularz zgłoszenia podatności

| Pole formularza | Opis / wymagane informacje |
|---|---|
| Dane zgłaszającego | Imię i nazwisko / nazwa podmiotu, e-mail, telefon (opcjonalnie). |
| Produkt | Nazwa, model, wersja sprzętowa, wersja firmware/oprogramowania. |
| Środowisko | Sposób instalacji, konfiguracja, sieć, usługa zdalna, moduł komunikacyjny. |
| Opis podatności | Opis problemu bezpieczeństwa i możliwego wpływu. |
| Kroki odtworzenia | Kolejne kroki pozwalające odtworzyć podatność. |
| Dowody techniczne | Logi, zrzuty ekranu, proof of concept, konfiguracja testowa. |
| Ocena wpływu | Wpływ na poufność, integralność, dostępność, autentyczność lub bezpieczeństwo pracy produktu. |
| Informacja o wykorzystaniu | Czy podatność jest lub może być aktywnie wykorzystywana. |
| Preferowana komunikacja | Adres kontaktowy, zgoda na publiczne podziękowanie, uwagi dot. koordynacji ujawnienia. |

# Załącznik nr 2. Minimalny zakres rejestru zgłoszeń podatności

| Kolumna rejestru | Opis |
|---|---|
| Numer sprawy | Unikalny identyfikator zgłoszenia. |
| Data wpływu | Data i godzina otrzymania zgłoszenia. |
| Źródło zgłoszenia | Badacz, klient, support, pracownik, dostawca, monitoring, inne. |
| Produkt / wersja | Nazwa produktu, model, wersja sprzętowa, firmware, aplikacja, usługa. |
| Opis podatności | Skrócony opis techniczny. |
| Priorytet | Krytyczny / wysoki / średni / niski. |
| Status | Nowe / w analizie / potwierdzone / poprawka / komunikacja / zamknięte / poza zakresem. |
| Właściciel sprawy | Osoba lub zespół odpowiedzialny za obsługę. |
| Działania | Decyzje, testy, poprawki, obejścia, komunikaty. |
| Raportowanie CRA | Informacja czy sprawa wymagała zgłoszenia oraz daty zgłoszeń. |
| Data zamknięcia | Data formalnego zamknięcia sprawy. |
| Wnioski | Działania zapobiegawcze i doskonalące. |

# Załącznik nr 3. Szablon komunikatu bezpieczeństwa

Tytuł: Komunikat bezpieczeństwa BRAGER nr [rok/numer]

- Produkt i wersje objęte komunikatem: [uzupełnić]
- Opis podatności: [opis bez ujawniania nadmiernych szczegółów technicznych]
- Poziom ryzyka: [krytyczny/wysoki/średni/niski]
- Potencjalny wpływ: [poufność/integralność/dostępność/autentyczność/bezpieczeństwo pracy]
- Dostępne działanie naprawcze: [aktualizacja/obejście/zmiana konfiguracji]
- Zalecenia dla użytkowników: [kroki działania]
- Data publikacji: [dd.mm.rrrr]
- Kontakt: security@brager.com.pl