

Regulamin zgłaszania podatności produktu

1. Cel

- Celem niniejszego Regulaminu jest określenie zasad zgłaszania, przetwarzania i postępowania w przypadku podejmowania działań mających na celu wykrycie w dobrej wierze podatności (ang. vulnerabilities) w Produktach BURY, zgodnie z polityką (https://www.bury.com/wp-content/uploads/2023/03/POLITYKA-CYBERBEZPIECZENSTWA-2021-11-08_EN.pdf). Nadrzędnym celem niniejszej regulacji jest zwiększenie poziomu bezpieczeństwa Produktów BURY.
- Aby ujawnianie podatności mogło zakończyć się sukcesem, warunkiem jest współpraca pomiędzy Zgłaszającym oraz BURY. Regulamin ma na celu określenie warunków komunikacji z uwzględnieniem podstaw prawnych oraz praw i obowiązków obowiązujących obydwie strony.

2. Definicje

- **BURY** – każda ze spółek powiązanych z GRUPY BURY będąca właścicielem, producentem lub zarządzającym Produktem, w którym występuje Podatność.
- **Produkt** – system i/lub urządzenie w tym rozwiązania technologiczne, które są wykorzystywane do prawidłowego i zamierzonego działania, przetwarzania, przechowywania lub transmisji danych oraz do zarządzania systemami informacyjnymi.
- **Podatność**: Słabość w Produkcie (czy to przez błąd w konfiguracji, czy w oprogramowaniu), która może zostać wykorzystana do przeprowadzenia nieautoryzowanych działań.
- **Zgłaszający**: osoba lub podmiot, który wyszukuje lub identyfikuje Podatność (tzw. etyczni hakerzy, badacze bezpieczeństwa) i/lub zgłasza Podatność.
- **Zespół ds. Bezpieczeństwa**: Dedykowany zespół w BURY odpowiedzialny za ocenę i usuwanie zgłoszonych Podatności - PSIRT (Product Security Incident Response Team – zespół ds. incydentów związanych z bezpieczeństwem produktów).

3. Zakres

- Regulamin dotyczy wszystkich Produktów oferowanych przez BURY.

4. Zgłaszanie Podatności

- Działania mające na celu wykrycie Podatności mogą być podejmowane wyłącznie w celu zabezpieczenia Produktu BURY, albo opracowania metody takiego zabezpieczenia.
- Działania w celu wykrycia Podatności nie mogą zostać zastosowane do jakichkolwiek czynności mających na celu naruszenie interesu publicznego lub prywatnego, dóbr osobistych, praw własności intelektualnej osób trzecich, działań o charakterze niszczącym lub wywołującymi szkody w Produktach, systemach, urządzeniach lub sieciach informatycznych oraz innych naruszeń prawa.
- Jeśli Zgłaszający zidentyfikuje potencjalną Podatność w Produkcie, należy ją niezwłocznie zgłosić zgodnie z poniższą procedurą:
- Zgłoszenie Podatności musi zostać skierowane bezpośrednio do BURY, dedykowanym kanałem Zgłoszenia, a nie za pośrednictwem przestrzeni publicznej jak np. fora internetowe lub media społecznościowe.
- **Dedykowany kanał Zgłoszenia**: Podatności mogą być zgłaszane poprzez dedykowany formularz na naszej stronie internetowej Wysłanie wiadomości na jakikolwiek inny kanał komunikacji może skutkować wydłużeniem czasu reakcji oraz nie zwalnia z obowiązku stosowania postanowień niniejszego Regulaminu.
- Zgłoszenie Podatności powinno zawierać następujące informacje:
 - szczegółowy opis Podatności,
 - informacje kontaktowe zgłaszającego (opcjonalnie),
 - zalecenia dotyczące naprawy podatności (opcjonalne).
- Dalsza korespondencja w sprawie będzie realizowana za pośrednictwem e-mail PSIRT@bury.com i powinna być szyfrowana z użyciem klucza publicznego dostępnego na stronie:

5. Procedura Postępowania po otrzymaniu Zgłoszenia

- **Potwierdzenie Otrzymania Zgłoszenia:**
 - Po otrzymaniu Zgłoszenia, Zgłoszenie zostanie dodane do listy a Zgłaszający otrzyma potwierdzenie odbioru Zgłoszenia w ciągu 48 godzin.
- **Weryfikacja Zgłoszenia:**
 - Zespół ds. Bezpieczeństwa przeprowadzi wstępną ocenę Zgłoszenia w ciągu 5 dni roboczych.
 - Jeżeli Zgłoszenie jest uzasadnione, zostanie nadany priorytet i plan działań naprawczych.
 - Zespół ds. Bezpieczeństwa poda proponowany termin opracowania rozwiązania. W razie odrzucenia Zgłoszenia opiszemy przyczyny takiego działania, ale pozostaniemy otwarci na nowe informacje w danej sprawie.
- **Konsultacje ze Zgłaszającym:**
 - W razie potrzeby, Zespół ds. Bezpieczeństwa może skontaktować się ze Zgłaszającym w celu uzyskania dodatkowych informacji.
- **Działania Naprawcze:**
 - Zespół ds. Bezpieczeństwa opracuje plan minimalizacji zagrożenia dla Produktów.
- **Zakończenie Procesu:**
 - Zgłaszający może zostać poproszony o zweryfikowanie, czy podatność została skutecznie usunięta.
 - Jeżeli Zgłaszający wyraził zgodę, może zostać uhonorowany na stronie Zgłaszania Podatności.

6. Zasady Etyki i Poufności

- Wszystkie informacje uzyskane i zgromadzone w ramach procesu Zgłaszania Podatności będą traktowane jako poufne i mogą być wykorzystywane wyłącznie do celów poprawy bezpieczeństwa Produktów. Ujawnienie informacji uzyskanych i/lub zgromadzonych w ramach procesu Zgłaszania Podatności (w tym jej wykrycia) może nastąpić wyłącznie po uzyskaniu uprzedniej pisemnej zgody BURY.
- Zasady etycznego Zgłaszania Podatności:
 - Zakazane jest wykorzystywanie Zgłoszonych Podatności przez Zgłaszającego oraz osoby trzecie.
 - Zakazane jest ujawnianie podatności przed jej Zgłoszeniem BURY.
 - Zakazane jest podejmowanie działań mających na celu szkodenia Produktom i/lub użytkownikom końcowym drogi.
 - Zakazane jest wykorzystywanie podatności w celu uzyskania nieuprawnionego dostępu do danych lub uszkodzenia danych.
 - Zakazane jest zamieszczanie, przekazywanie, wgrywanie, wysyłanie, przechowywanie lub zamieszczanie odnośników do złośliwego oprogramowania.
 - Zakazane jest przeprowadzanie prób, które mogą doprowadzić do rozesłania niepożądanych albo nieautoryzowanych wiadomości, spamu lub innej formy niepożądanej korespondencji lub treści niezgodnych z prawem.
 - Zakazane jest naruszanie praw osób trzecich w celu wykrycia Podatności.

7. Ochrona Zgłaszającego

- BURY zobowiązuje się nie podejmować działań prawnych przeciwko Zgłaszającym Podatności w dobrej wierze, zgodnie z niniejszym Regulaminem.
- Każde Zgłoszenie podlega ochronie przed udostępnieniem osobom nieuprawnionym. Informacje objęte Zgłoszeniem, umożliwiające identyfikację osoby dokonującej Zgłoszenie, będą chronione zarówno na etapie wyjaśniania sprawy, podczas prowadzenia ewentualnych działań zapobiegawczych, jak również w przyszłości i udostępniane wyłącznie uprawnionym osobom i podmiotom.

- Zgłaszający może pozostać anonimowy, jeśli tego sobie życzy.

8. Prawa własności intelektualnej

- Zgłaszający z chwilą przekazania Zgłoszenia, bez wynagrodzenia, przenosi na BURY przysługujące Zgłaszającemu majątkowe prawa autorskie do całości jak i poszczególnych (części) utworów (wszelkich rezultatów wykrytych Podatności oraz rezultatów wykonanych Zgłoszeń) dostarczonych BURY w ramach wykonanego Zgłoszenia, bez jakichkolwiek ograniczeń terytorialnych, czasowych czy ilościowych, na wszelkich znanych polach eksploatacji w dacie Zgłoszenia, w tym wymienionych w art. 50 i art. 74 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, w szczególności:
 - w zakresie utrwalania i zwielokrotniania utworu - wytwarzania dowolną techniką egzemplarzy utworu, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
 - tłumaczenia, przystosowywania, zmiany układu lub wprowadzanie jakichkolwiek innych zmian w utworach;
 - w zakresie obrotu oryginałem albo egzemplarzami, na których utwór utrwalono - wprowadzanie do obrotu, użyczenie lub najem oryginału albo egzemplarzy, wprowadzanie do Produktów;
 - w zakresie rozpowszechniania utworu w sposób inny niż określony w punkcie poprzedzającym – publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym;
 - wykorzystywanie utworu do celów marketingowych lub promocji, w tym reklamy, sponsoringu, promocji sprzedaży, a także do oznaczenia lub identyfikacji produktów i usług oraz innych przejawów działalności, a także dla celów edukacyjnych lub szkoleniowych.
- Zgłaszający zobowiązuje się nie wykonywać przysługujących mu autorskich praw osobistych do utworów lub poszczególnych ich elementów, ani że nie będzie zgłaszać wobec BURY lub podmiotów upoważnionych przez BURY do korzystania z utworów oraz jego następców prawnych jakichkolwiek roszczeń z tytułu naruszenia przez BURY lub przez podmioty upoważnione przez BURY, lub jego następców prawnych autorskich praw osobistych do utworów.

9. Nagrody za Zgłoszenie Podatności

- **Obecnie BURY nie prowadzi ustalonego z góry programu “bug bounty” ani nie uczestniczy w takim programie. BURY nie honoruje wniosków o zapłatę za Zgłoszenie Podatności, poza indywidualnie przyznanymi w sposób uznaniowy przypadkami.**
- BURY może zdecydować o przyznaniu nagrody dla Zgłaszającego, który jako pierwszy zgłosi istotną podatność.
- Wysokość i forma nagrody są ustalane uznaniowo i indywidualnie.

10. Zmiany Regulaminu

- BURY zastrzega sobie prawo do wprowadzania zmian w niniejszym Regulaminie. O wszelkich zmianach Zgłaszający będą informowani na stronie internetowej BURY.

11. Kontakt

- Wszelkie pytania dotyczące niniejszego regulaminu należy kierować na adres: PSIRT@bury.com