Politique de Divulgation responsable des Vulnérabilités

1. Vue d'ensemble

1.1 Objectif

Batopin SA s'engage à fournir au grand public des systèmes et des services sécurisés en mettant en œuvre des mesures et des processus de sécurité appropriés pour protéger les informations qu'elle traite. Bien que nous nous efforcions de maintenir un niveau élevé de sécurité, des vulnérabilités peuvent subsister.
La présente politique a pour objectif de fournir à toute personne disposant des compétences requises un cadre clair pour identifier et signaler de manière responsable d'éventuelles vulnérabilités de sécurité. Elle définit également la procédure de transmission à Batopin SA des informations sur les vulnérabilités, afin de nous permettre d'examiner, de valider et de traiter les problèmes de sécurité signalés.

1.2 Champ d'application

La présente Politique s'applique à toutes les vulnérabilités de sécurité de l'information identifiées par des tiers dans :
• les interfaces accessibles au public des distributeurs automatiques de billets exploités par Batopin
• cash.be
• batopin.be
Les autres systèmes gérés ou utilisés par Batopin sont expressément exclus du champ d'application et ne peuvent faire l'objet de tests dans le cadre de la présente politique.

2. Politique de Divulgation des Vulnérabilités

2.1 Investigation

À condition que vous agissiez de bonne foi, que vous respectiez le champ d'application, les conditions et les restrictions de la présente politique, ainsi que l'ensemble des lois et réglementations applicables, Batopin n'a pas l'intention d'engager une action en justice à votre encontre en lien avec vos investigations sur les vulnérabilités.

2.1.1 Conditions générales

Les conditions suivantes doivent être respectées lors d'une investigation de sécurité sur les systèmes autorisés :

- Informer Batopin dès que possible après avoir identifié une vulnérabilité de sécurité ;
- Ne pas exploiter les vulnérabilités au-delà de ce qui est strictement nécessaire pour démontrer la vulnérabilité. La proportionnalité doit être respectée : si la vulnérabilité peut être démontrée sur un cas limité, aucune action supplémentaire ne doit être entreprise ;
- Ne partager l'accès avec personne ;
- Cesser immédiatement les tests et signaler la vulnérabilité si des informations sur les clients, des données à caractère personnel, des données d'authentification, des données de transaction ou d'autres informations confidentielles deviennent accessibles ;
- Les tests doivent être réalisés de manière à éviter toute perturbation, dégradation ou interruption des services et systèmes de Batopin ;
- Toute porte dérobée, tout accès et tout mécanisme de persistance doivent être supprimés une fois la vulnérabilité démontrée.

2.1.2 Actions interdites

Les actions suivantes sont strictement interdites durant l'investigation :

- Accéder à des données, les traiter ou les copier, sauf dans la mesure strictement nécessaire à votre investigation. À l'issue de l'investigation, les données doivent être définitivement détruites ;
- Modifier, supprimer ou endommager de toute autre manière des données et des systèmes ;
- Installer des logiciels malveillants ;
- Toute technique ayant pour seul objectif d'affecter la disponibilité de nos systèmes et services, telle que les attaques par déni de service (distribué) ((D)DOS), les tests de charge et les tests de résistance ;
- Toute tentative de contournement des contrôles de sécurité physique ;
- Les attaques d'ingénierie sociale et d'hameçonnage ;
- L'envoi de messages indésirables ;
- Le vol de mots de passe ou les techniques de force brute ;

- Le vandalisme ;
- Toute tentative de distribution d'espèces, de modification de transactions, d'interférence avec le traitement des transactions ou de toute autre atteinte aux opérations financières.

2.1.3 Confidentialité

Les tiers doivent traiter toutes les informations obtenues durant l'investigation comme strictement confidentielles et ne doivent ni les partager, ni les divulguer, ni les utiliser de toute autre manière à d'autres fins que le signalement de la vulnérabilité à Batopin.

Si la vulnérabilité est susceptible d'affecter également d'autres organisations en Belgique, le tiers responsable peut en informer le Centre pour la Cybersécurité Belgique sans révéler d'informations détaillées concernant Batopin.

La divulgation publique, la publication, les discussions sur les réseaux sociaux, les présentations lors de conférences ou le partage de détails sur les vulnérabilités avec d'autres parties ne sont pas autorisés, sauf si Batopin a confirmé la correction ou donné son autorisation écrite préalable.

Après confirmation de la correction par Batopin ou obtention d'une autorisation écrite préalable, l'auteur du signalement peut divulguer publiquement l'existence de la vulnérabilité, à condition que :

- Batopin soit informée au préalable de la divulgation envisagée ;
- La divulgation ne contienne aucun code d'exploitation, code de preuve de concept, instruction d'attaque détaillée, détail de configuration, capture d'écran ou autre information pouvant raisonnablement faciliter l'exploitation de la vulnérabilité ;
- Aucune information confidentielle, donnée à caractère personnel, information sur les clients ou autre information sensible en matière de sécurité concernant Batopin ne soit divulguée ;
- La divulgation respecte l'ensemble des lois et réglementations applicables.

2.2 Signalement

Les tiers, y compris les chercheurs en sécurité et les hackers éthiques, sont encouragés à signaler les vulnérabilités identifiées à security@batopin.be. Les signalements peuvent être anonymes. Si des coordonnées sont communiquées, un accusé de réception de votre signalement sera envoyé.

À la demande du tiers, Batopin fournira un lien sécurisé permettant de déposer le rapport de vulnérabilité dans un espace sécurisé géré par Batopin.

Lors du signalement d'une vulnérabilité, nous vous recommandons de fournir :

- Une description de la vulnérabilité
- Les étapes permettant de reproduire le problème (des scripts ou des captures d'écran sont utiles)
- L'impact potentiel
- L'emplacement de la vulnérabilité

Nous vous prions de soumettre les rapports en anglais.

Dans la mesure de ses moyens et lorsque la loi le permet, Batopin confirmera l'existence de la vulnérabilité.

Batopin a pour objectifs de :

- Accuser réception des signalements de vulnérabilités dans un délai de 5 jours ouvrés ;
- Procéder à une évaluation initiale du signalement ;
- Fournir, le cas échéant, des informations sur l'avancement de l'investigation ;
- Échanger avec l'auteur du signalement lorsque des informations supplémentaires sont nécessaires.

Ces objectifs sont indicatifs et ne constituent pas des engagements contraignants.

2.3 Récompenses

Batopin ne propose actuellement aucun programme de récompense pour les vulnérabilités ni de prime aux bogues. Batopin peut, à sa seule discrétion, témoigner sa reconnaissance pour les signalements valides. Une telle reconnaissance n'est pas garantie et est évaluée au cas par cas.

2.4 Questions

Les questions concernant la présente politique peuvent être envoyées à security@batopin.be. Nous vous invitons également à nous faire part de vos suggestions pour améliorer cette politique.