Politique de Divulgation des Vulnérabilités

Date d'entrée en vigueur : 25 mars 2025

1. Introduction

Staples s'engage à assurer la sécurité de ses clients ainsi que des informations qu'ils partagent avec nous via nos plateformes et services en ligne. Nous reconnaissons également l'apport précieux des chercheurs en sécurité dans l'identification des vulnérabilités et préoccupations en cybersécurité. Cette politique vise à fournir des lignes directrices claires pour la découverte de vulnérabilités et à expliquer comment soumettre celles qui sont découvertes.

2. Conformité

Si vous agissez de bonne foi et respectez cette politique, Staples s'engage à ne pas engager de poursuites judiciaires ni à signaler l'incident aux autorités. Toute ambiguïté sera interprétée en faveur des chercheurs en sécurité agissant de manière éthique et responsable.

3. Exigences

Cette politique exige que vous :

- Nous avisiez dès que possible après avoir découvert un problème de sécurité réel ou potentiel ;
- Preniez toutes les mesures nécessaires pour éviter les atteintes à la vie privée, la dégradation de l'expérience utilisateur, les interruptions de service ou la destruction ou manipulation de données ;
- Utilisiez les exploits uniquement dans la mesure nécessaire pour confirmer la présence d'une vulnérabilité — sans collecter, modifier ou supprimer de données, établir un accès persistant ou tester d'autres systèmes, réseaux ou applications ;
- Ne divulguiez aucun détail concernant une vulnérabilité présumée à des tiers sans le consentement écrit exprès de Staples — toute divulgation non autorisée sera considérée comme non conforme à cette politique.

Dès que vous avez confirmé l'existence d'une vulnérabilité ou accédé à des données confidentielles ou sensibles (y compris des renseignements personnels, financiers ou exclusifs), **vous devez immédiatement cesser vos tests, nous en informer et ne pas divulguer ces données.**

4. Méthodes de Test Interdites

Les méthodes de test suivantes ne sont pas autorisées :

- Tests de déni de service (DoS ou DDoS) ou tout autre test pouvant nuire à l'accès ou endommager les systèmes, réseaux, applications ou données, même temporairement ;
- Accès, téléchargement ou modification de données dans un compte qui ne vous appartient pas ;
- Tests entraînant l'envoi de courriels, messages texte, appels téléphoniques ou autres communications non sollicitées à des tiers — y compris les associés, clients ou partenaires de Staples ;
- Ingénierie sociale, y compris la fausse représentation de Staples ou de son personnel ;
- Intrusion physique ou tests liés à la sécurité physique ;
- Publication, transmission, téléchargement, lien ou stockage de logiciels malveillants ;
- Tests sur des systèmes, réseaux, applications ou services tiers, même s'ils sont exploités pour le compte de Staples.

5. Portée

Cette politique s'applique aux sites Web et services suivants de la famille Staples :

- Staples.com
- StaplesConnect.com
- StaplesAdvantage.com
- StaplesPromotionalProducts.com
- Quill.com
- HiTouchBusinessServices.com
- ediversitynetwork.com
- SouthwestOrdering.com
- app.staplespay.com

Les tests autorisés dans le cadre de cette politique sont strictement limités aux applications Web énumérées ci-dessus. L'infrastructure réseau, les systèmes internes et les services tiers (y compris les environnements infonuagiques) sont exclus de la portée. Si vous croyez qu'un problème de sécurité existe en dehors de cette portée mais affecte Staples, veuillez nous contacter à l'adresse suivante avant d'effectuer tout test : vulnerabilityreport@staples.com.

Cette portée peut être mise à jour, et nous encourageons les chercheurs à la consulter régulièrement.

6. Signalement d'une Vulnérabilité

Les rapports de vulnérabilités peuvent être envoyés par courriel à : vulnerabilityreport@staples.com. Les soumissions anonymes sont acceptées.

Ce que nous aimerions recevoir de votre part

Pour nous aider à prioriser les soumissions, votre rapport devrait idéalement :

- Décrire en détail la vulnérabilité et son emplacement ;
- Fournir des instructions étape par étape pour valider et reproduire la découverte ;
- Inclure tout script de preuve de concept ou artefact pertinent (captures d'écran, etc.).

Ce que vous pouvez attendre de nous

Si vous soumettez une vulnérabilité valide en conformité avec cette politique, nous nous engageons à :

- Accuser réception du rapport dans un délai de 5 jours ouvrables ;
- Communiquer avec vous pour comprendre et valider le problème, si nécessaire ;
- Traiter la vulnérabilité de manière appropriée, selon l'évaluation de Staples.

Veuillez noter que Staples n'offre pas de programme de récompense pour les bogues (« bug bounty ») et n'offre aucune compensation pour les soumissions.

Staples se réserve le droit de modifier ou de mettre fin à cette politique à tout moment.

7. Questions

Si vous avez des doutes concernant la portée, les méthodes de test acceptables ou toute autre disposition de cette politique, nous vous encourageons à nous contacter à vulnerabilityreport@staples.com.
Nous vous invitons également à nous faire part de vos suggestions pour améliorer cette politique.