HGF Limited

Politique de divulgation des vulnérabilités

Public

Propriétaire du document	Responsable des operations informatiques & sécurité
Audience	Public – chercheurs en sécurité, clients, fournisseurs, members du public
Version	1.0
Date d'entrée en vigueur	[à confirmer lors de la publication]
Cycle de revision	Annuel, ou plus tôt en cas de changement substantiels
Contact	security@hgf.com

1. Introduction

HGF Limited (« HGF », « nous », « notre ») attache une grande importance à la sécurité de ses systèmes, des informations de ses clients ainsi que du public au sens large. Nous accueillons favorablement les signalements de la communauté des chercheurs en sécurité ainsi que des membres du public qui identifient des vulnérabilités potentielles dans nos produits, services ou infrastructures.
Cette politique explique comment nous signaler une vulnérabilité, ce que vous pouvez attendre de notre part en retour et les conditions dans lesquelles les chercheurs sont invités à intervenir. Elle est conçue pour s'aligner sur les principes des normes ISO/IEC 29147 (divulgation des vulnérabilités), ISO/IEC 30111 (gestion des vulnérabilités) et sur le Toolkit de divulgation des vulnérabilités du National Cyber Security Centre du Royaume-Uni.

2. Champs d'application

Dans le champs d'application

Cette politique s'applique aux vulnérabilités découvertes dans tout système accessible au public appartenant à ou exploité par HGF Limited, y compris, sans s'y limiter :

- Notre site principal et tous les sous-domaines de hgf.com
- Les portails clients, extranets et services d'échange de documents exploités par HGF
- Les services de messagerie et d'authentification lorsque des erreurs de configuration sont observables depuis l'extérieur

• Les applications mobiles ou web publiées par HGF sous son propre nom**Hors champs d'application**

Les éléments suivants sont explicitement exclus et ne doivent pas être testés ni signalés dans le cadre de cette politique :

- Les services, plateformes ou sites web tiers non exploités par HGF (veuillez les signaler au fournisseur concerné)
- Les attaques physiques contre les bureaux, le personnel ou les biens de HGF
- L'ingénierie sociale visant le personnel, les clients ou les sous-traitants de HGF (y compris le phishing, le vishing ou le pretexting)
- Les attaques par déni de service, les tests volumétriques ou toute activité susceptible de dégrader le service pour d'autres utilisateurs
- Les constats issus de scanners automatisés sans impact démontrable sur la sécurité (par ex. en-têtes de sécurité manquants sans exploitation possible)
- Les signalements de versions logicielles obsolètes sans preuve de concept fonctionnelle
- Les problèmes liés aux normes de messagerie (SPF, DKIM, DMARC) sans exploitation active démontrée
- Le self-XSS, le clickjacking sur des pages sans actions sensibles ou d'autres problèmes théoriques à faible impact

3. Comment signaler une vulnérabilité

Si vous pensez avoir identifié une vulnérabilité de sécurité dans un système relevant du périmètre, veuillez nous contacter à l'adresse suivante : security@hgf.com.

Afin de nous aider à analyser et traiter votre signalementle plus rapidement possible, veuillez inclure :

- Une description claire de la vulnérabilité et de son impact potential
- L'URL, le point de terminaison ou le système affecté
- Les étapes de reproduction détaillées, y compris toute charge utile ou script necessaire
- Des captures d'écran, des enregistrements requête/réponse ou du code de preuve de concept si utile
- Votre nom ou pseudonyme (si vous souhaitez être crédité) et un moyen de contact privilégié

Les rapports peuvent être soumis en anglais. Nous acceptons les signalements anonymes, mais cela peut limiter notre capacité à poser des questions de suivi ou à reconnaître votre contribution.

4. Nos engagements envers vous

Lorsque vous soumettez un rapport de bonne foi et conformément à cette politique, HGF s'engage à :

- **Accusé de réception** : accuser réception de votre rapport dans un délai de cinq (5) jours ouvrables au Royaume-Uni
- **Qualification** : valider et évaluer le rapport et fournir une première réponse dans un délai de dix (10) jours ouvrables au Royaume-Uni

- **Communication** : vous tenir informé de l'avancement à des intervalles raisonnables pendant l'enquête et la remediation
- **Résolution** : corriger les vulnérabilités confirmées dans un délai proportionné à leur gravité, généralement dans les 90 jours pour les cas élevés ou critiques
- **Reconnaissance** : avec votre consentement, reconnaître votre contribution. HGF ne propose pas actuellement de programme de bug bounty rémunéré
- **Safe harbour** : voir section 6 ci-dessous5. Ce que nous attendons de vous

5. Ce que nous attendons de vous

Afin de protéger nos clients, notre personnel et l'intégrité de toute enquête, nous demandons aux chercheurs agissant dans le cadre de cette politique :

- De faire preuvre de bonne foi et éviter toute atteinte à la vie privée, toute dégradation de l'expérience utilisateur, perturbation des systèmes de production ou destruction/modification de données
- D'interagir uniquement avec des comptes leur appartenant ou avec l'autorisation explicite du titulaire
- De ne pas accéder, modifier, conserver ou partager des données appartenant à HGF, à nos clients ou à d'autres utilisateurs au-delà de ce qui est strictement nécessaire pour démontrer la vulnérabilité
- D'arrêter les tests et de nous contacter immédiatement en cas de présence de données personnelles, d'informations confidentielles clients ou d'indication de compromission existante
- De laisser à HGF un délai raisonnable pour enquêter et corriger avant toute divulgation publique (nous demandons généralement un délai coordonné de 90 jours à compter de l'accusé de réception)
- De ne pas recourir à l'extorsion, à des menaces ni à toute tentative d'exploitation commerciale des résultats en dehors de cette politique

6. Safe Harbour

HGF considère les activités de recherche en sécurité et de divulgation des vulnérabilités menées conformément à cette politique comme autorisées. Nous n'engagerons pas de poursuites civiles ni de plainte auprès des autorités contre les chercheurs qui :

- Agissent de bonne foi et respectent les conditions de cette politique
- N'exploitent pas la vulnérabilité au-delà de ce qui est nécessaire pour en confirmer l'existence
- Signalent rapidement la vulnérabilité à HGF et ne la divulguent pas publiquement avant sa correction convenue

Si une action en justice est engagée contre vous par un tiers pour des activités menées conformément à cette politique, nous prendrons des mesures raisonnables pour indiquer que vos actions étaient autorisées dans le cadre de ce programme.

Cette clause de protection ne s'applique pas aux activités malveillantes, illégales ou hors périmètre de cette politique. HGF se réserve le droit de prendre toute mesure appropriée pour protéger ses systèmes, son personnel et ses clients, y compris le signalement aux autorités, lorsque les activités dépassent ce cadre.

7. Confidentialité et données personnelles

Les informations que vous fournissez dans le cadre d'un signalement seront traitées conformément à l'Avis de confidentialité de HGF et aux lois applicables en matière de protection des données, y compris le RGPD britannique et le Data Protection Act 2018. Nous utiliserons ces informations uniquement aux fins d'enquête, de résolution et, le cas échéant, de divulgation de la vulnérabilité signalée.

Nous demandons aux chercheurs de ne pas inclure de données personnelles clients, d'informations confidentielles ni d'identifiants tiers dans leurs rapports. Si de telles informations sont rencontrées lors des tests, elles ne doivent pas être conservées, copiées ni partagées et doivent être signalées immédiatement à HGF.

8. Divulgation coordonnée de vulnérabilités (CVD)

HGF soutient le principe de divulgation coordonnée des vulnérabilités. Lorsqu'un chercheur souhaite publier des détails d'une vulnérabilité confirmée, nous demandons que la publication soit différée jusqu'à la mise en place de correctifs et la notification des parties concernées, généralement dans les 90 jours suivant l'accusé de réception. Nous sommes disposés à coordonner toute communication publique conjointe sur demande.

9. Maintenance de la politique

Cette politique sera revue au moins annuellement par le Responsable des opérations informatiques & sécurité, ou plus tôt en cas de changement significatif des services, du paysage des menaces ou de la réglementation. La version actuelle est publiée à https://hgf.com/security.

Contrôle du document
Responsable : Responsable des opérations informatiques & sécurité • **Classification** : Public • **Version** : 1.0