MODIFICATION SUMMARY

Version	Résumé des Changements	Ecrit par	Vérifié par	Approuvé par	Date
A	Creation	C. Mace			

Sommaire

1. Introduction et Objectif

Notre entreprise s'engage à maintenir un environnement de sécurité robuste pour nos clients et utilisateurs. Nous reconnaissons l'importance d'une collaboration responsable et transparente avec la communauté de sécurité informatique pour identifier et résoudre les vulnérabilités de manière efficace.

Cette politique établit un cadre de divulgation coordonnée qui permet aux chercheurs en sécurité de nous contacter et de signaler les vulnérabilités de manière responsable, tout en protégeant nos utilisateurs et en maintenant la confidentialité des informations sensibles.

Dans le cadre de cette divulgation coordonnée, le rapport initial est d'abord fait en privé à l'entreprise et rendu public après un délai précisé dans ce document dans une communication coordonnée avec le ou les chercheurs ayant signalé la vulnérabilité.

2. Définitions

Vulnérabilité : Une faiblesse dans nos systèmes, applications ou processus qui pourrait être exploitée pour compromettre la confidentialité, l'intégrité ou la disponibilité des données ou des services.

Chercheur en Sécurité : Toute personne ou organisation qui découvre et signale une vulnérabilité de manière responsable.

Divulgation Coordonnée : Un processus où le chercheur signale la vulnérabilité à notre équipe, qui dispose d'un délai défini pour développer et déployer un correctif avant une divulgation publique.

Divulgation Publique : La publication des détails de la vulnérabilité après que les corrections aient été mises en œuvre ou après l'expiration des délais convenus.

3. Processus de Signalement

3.1 Comment Signaler une Vulnérabilité

- Envoyez un rapport détaillé à : security@livingpackets.com
- Pour une confidentialité accrue, chiffrez votre rapport avec notre clé PGP publique (disponible sur demande)

3.2 Contenu du Rapport Idéal

- Description détaillée de la vulnérabilité et de son impact
- Étapes pour reproduire le problème (requêtes HTTP, captures d'écrans ou autre détails)
- Version(s) affectée(s) du produit
- Preuve de concept ou démonstration (si possible)
- Informations de contact du chercheur

4. Calendrier et Délais

Étape	Délai
Accusé de réception	Dans les 72 heures suivant la réception
Confirmation et évaluation	Dans les 5 jours ouvrables
Développement du correctif	Variable selon la complexité
Délai de divulgation coordonnée	90 jours maximum après mise à jour

5. Communication et Coordination

5.1 Points de Contact

- E-mail : security@livingpackets.com
- Formulaire web :
- Responsable de la Sécurité : [Clément Macé, security@livingpackets.com]

5.2 Langage de Communication

Nous communiquons en français et en anglais. Veuillez indiquer votre préférence dans votre rapport initial.

Nous maintiendrons une communication régulière avec le chercheur tout au long du processus, avec des mises à jour au minimum toutes les deux semaines.

5.3 Conduite Attendue

- Ne pas accéder à plus de données que nécessaire pour démontrer la vulnérabilité
- Ne pas modifier ou supprimer de données
- Ne pas déranger les opérations ou services
- Respecter les délais de divulgation coordonnée convenus

6. Confidentialité et Respect de la Vie Privée

- Nous ne divulguerons pas l'identité du chercheur sans consentement
- Les informations partagées dans les rapports de vulnérabilité sont traitées de manière confidentielle
- Les données personnelles du chercheur sont protégées conformément à la législation applicable (RGPD)
- Les informations seront divulguées en interne uniquement à ceux qui ont besoin de connaître ces éléments

7. Processus de Divulgation Publique

1. **Timing :** Une divulgation publique ne sera effectuée qu'après que le correctif ait été déployé, ou 90 jours après la notification initiale, selon la première occurrence
2. **Coordination :** Nous coordonnerons avec le chercheur sur le texte de divulgation publique
3. **Reconnaissance :** Avec autorisation, nous mentionnerons le chercheur dans nos annonces de sécurité
4. **Exceptions :** Si nous découvrons une exploitation active, nous pouvons accélérer la divulgation

8. Exclusions et Limitations

Nous ne sommes pas en mesure d'accepter les rapports pour :

- Les problèmes de configuration des clients (mauvais paramétrage par l'utilisateur)
- Les problèmes affectant les versions obsolètes ou non supportées
- Les problèmes physiques ou de sécurité des locaux
- Le spam ou les attaques par déni de service
- Les problèmes découlant d'une mauvaise utilisation ou d'une non-conformité aux conditions d'utilisation

9. Protection Légale

Nous n'entamerons pas de procédures judiciaires contre les chercheurs en sécurité qui signalent les vulnérabilités de bonne foi et en conformité avec cette politique. Cela inclut l'accès temporaire aux systèmes pour démontrer la vulnérabilité, à condition que le chercheur n'accède à aucune donnée au-delà du nécessaire pour la démonstration.

10. Amélioration Continue

Nous examinons régulièrement cette politique et recueillons les commentaires des chercheurs en sécurité. Si vous avez des suggestions pour améliorer ce processus, veuillez les adresser à notre équipe de sécurité.

Dernière mise à jour : 09/07/2026

Responsable de la Sécurité
Nom complet : Clément Macé
Titre : Data Protection Officer