Politique de divulgation de vulnérabilités
Programme de *bug-bounty*

FICHE DE SUIVI

DESCRIPTION	
Objet	Politique de divulgation de vulnérabilités
Version	1.0
Auteur	CAM (RSSI)
Statut	PUBLIÉ
Contrôles ISO/IEC27002:2022	8.8

REVISION			
Version	**Date**	**Auteur**	**Commentaire**
1.0	2022-09-27	CAM (RSSI)	Création

VALIDATION	
Version	**Visa électronique**
1.0	CEO Antoine Plantier Certified by yousign

Les versions précédemment approuvées sont conservées par la Sécurité de SharingCloud.

TABLE DES MATIÈRES

1 CONTEXTE ET PÉRIMÈTRE

SharingCloud est un expert européen, créateur de solutions de Smart Office pour accompagner les nouvelles façons de travailler.

Notre plateforme logicielle Instant Suite® digitalise les espaces afin d'optimiser les bâtiments, ainsi que le travail hybride pour l'ensemble des collaborateurs.

Aménagement de bureaux partagés, gestion intelligente des salles de réunion, simplification du parcours des collaborateurs et des invités, mise en place et suivi efficace du télétravail, communication, réduction de l'empreinte écologique des bâtiments, réduction des coûts immobiliers…

Personnalisables et sécurisées, nos solutions de Smart Office s'ajustent aux besoins de tous les types d'entreprises et permettent de gérer au mieux le bon fonctionnement des politiques de Smart Office.

Néanmoins, malgré tous nos efforts, il reste possible que des vulnérabilités nous échappent dans nos produits.

Ce document décrit la politique de SharingCloud pour ce qui concerne la divulgation organisée de vulnérabilités par des tiers.

Nous acceptons les rapports de toutes les bonnes volontés : chercheurs, *bounty hunters*, CERTs, …, désignées par la suite par le terme « chercheur ». Des exceptions sont toutefois prévues au chapitre 5 ci-dessous.

SharingCloud implémente la RFC 9116 relative au signalement de vulnérabilités. Ainsi, cette politique est reprise dans notre fichier https://sharingcloud.com/.well-known/security.txt.

En cas de conflit entre ce fichier et cette politique, la politique prévaut.

2 COMMENT SIGNALER UNE VULNÉRABILITÉ

Les signalements se font par email à l'adresse security@sharingcloud.com.

Le rapport doit être rédigé en français ou en anglais, et contenir au moins les informations suivantes :

- Heure et date de la découverte, en précisant le fuseau horaire
- Préciser le contexte technique : navigateur et sa version, outils utilisés, etc.
- La ou les URL vulnérables
- La marche à suivre nécessaires pour reproduire l'exploitation
- Le cas échéant le plan actuel de divulgation
- Un point de contact : nom ou pseudo et adresse email.

À l'exception des coordonnées du chercheur, merci de n'inclure aucune donnée à caractère personnel.

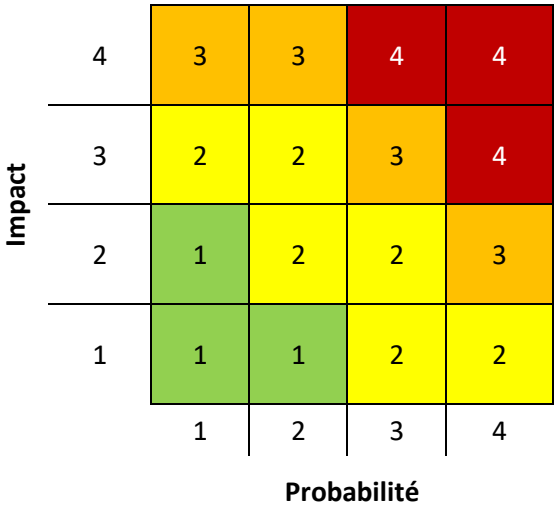
SharingCloud pourra utiliser comme il l'entend les informations du rapport de vulnérabilité fourni par le chercheur, à l'exception de son identité.

3 TRAITEMENT PAR SHARINGCLOUD

SharingCloud accusera réception de chaque rapport sous 5 jours ouvrés. Passé ce délai, un chercheur qui n'aurait pas été recontacté est invité à se manifester à nouveau.

Les équipes de SharingCloud évalueront chaque rapport pour déterminer la criticité des vulnérabilités détectées, sur la base de la formule suivante :

$Criticité = I \times P$, avec I l'impact estimé et P la probabilité d'occurrence



Légende	
4	Critique
3	Majeure
2	Moyenne
1	Mineure

Une fois que la vulnérabilité corrigée, SharingCloud pourra autoriser explicitement et par écrit le chercheur à rendre publique sa découverte s'il le souhaite.

Sans accord de publication, le chercheur s'engage à ne pas divulguer sa découverte.

4 RÉCOMPENSES

SharingCloud récompense les chercheurs en fonction de la criticité des vulnérabilités remontées, lorsque cette politique est totalement respectée.

Criticité	Récompense
Critique	1000 euros, *acknowledgment* sur notre page dédiée*
Majeure	400 euros, *acknowledgment* sur notre page dédiée*
Moyenne	*Acknowledgment* sur notre page dédiée*
Mineure	Aucune

** avec l'accord du chercheur sous l'identité ou pseudonyme de son choix, en tant que « Anonyme » le cas échéant.*

Les vulnérabilités déjà identifiées par SharingCloud ne peuvent donner lieu à une récompense.

Les récompenses financières sont transférées par virement bancaire en euros.

5 EXCLUSIONS

SharingCloud autorise les chercheurs à rechercher des vulnérabilités sur ses produits. Néanmoins, les cibles ou procédés suivants sont hors limites.

- Les clients, sous-traitants et partenaires de SharingCloud
- Les attaques par force brute, déni de service, ingénierie sociale
- Les actions destructives
- Les attaques sur la sécurité physique ou environnementale

Un chercheur ne respectant pas ces exclusions ne bénéficierait alors pas de la protection de cette politique et s'exposerait à des poursuites judiciaires.

Les salariés, clients, sous-traitants, revendeurs et partenaires technologiques de SharingCloud, sa maison-mère SharingGroup et ses filiales ne sont pas éligibles à ce programme de *bug bouty*. Il est rappelé que les audits et tests d'intrusion menés par des clients sont régis par le contrat de licence entre SharingCloud et le client et non par cette politique.

Lorsqu'une récompense financière est accordée, SharingCloud est soumis aux obligations légales en vigueur en France. Ainsi, certains pays et/ou certaines personnes ou organisations peuvent ne pas être éligibles et la récompense est alors définitivement perdue.

6 CONDITIONS GÉNÉRALES

SharingCloud s'engage à ne pas poursuivre le chercheur en justice sur la base des articles 323-1 et suivants du Code pénal pour les vulnérabilités signalées, aux conditions cumulatives que :

- les recherches sont effectuées sans perturber les activités de SharingCloud, ses clients et/ou ses sous-traitants ;
- le chercheur n'utilise ni ne modifie aucune des données ainsi découvertes ;
- le chercheur se conforme aux lois applicables en France et dans son pays ;
- le chercheur se conforme sans réserve à la présente politique.

SharingCloud s'engage à examiner pour chaque vulnérabilité la possibilité pour le chercheur de divulguer ses découvertes mais se réserve le droit de le refuser.

De manière générale, cette politique peut être mise à jour à tout moment sans préavis. Seule la dernière version publiée par SharingCloud, dans sa version française, fait foi. Il appartient aux chercheurs de s'assurer qu'ils possèdent la dernière version applicable.

En fonction des circonstances, SharingCloud se réserve le droit d'apporter des exceptions à cette politique (notamment les récompenses).

SharingCloud ne tentera qu'un seul virement bancaire par récompense. Il appartient au chercheur de s'assurer que ses coordonnées bancaires sont correctes.

- FIN DU DOCUMENT -