1 POLITIQUE DE DIVULGATION RESPONSABLE

Sisal veillera à ce que son système de gestion pour la sécurité des informations soit conforme à ce qui est prévu par les normes ISO/IEC 27001 et WLA SCS-2020. Sisal demande à tous les chercheurs en sécurité de contribuer à la signalisation d'éventuelles vulnérabilités que ces derniers ont pu détecter sur les produits et services SISAL afin de protéger au mieux les utilisateurs et leurs données.
Tous les chercheurs en sécurité pourront se familiariser avec les modalités de signalisation des vulnérabilités grâce à la présente politique.

1.1 Signalisation de vulnérabilité

Pour signaler une vulnérabilité à Sisal, il est possible d'envoyer un e-mail à :
responsible-disclosure@sisal.it

Afin de garantir la confidentialité des informations, il est demandé de chiffrer le contenu de l'e-mail via la clé PGP prévue à cet effet :

-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: User-ID: Sisal Responsible Disclosure <responsible-disclosure@sisal.it>
Comment: Created: 9/27/2022 5:08 PM
Comment: Expires: 9/27/2024 12:00 PM
Comment: Type: 255-bit EdDSA (secret key available)
Comment: Usage: Signing, Encryption, Certifying User-IDs
Comment: Fingerprint: 8DD59416803AADBBC11BAB77F5F64CEF2B962428

mDMEYzMR+RYJKwYBBAHaRw8BAQdAv9zZlzLchOeKqnEQlWYXtMGAxy1Uegl4643a
lvMQJmy0PlNpc2FsIFJlc3BvbnNpYmxlIERpc2Nsb3N1cmUgPHJlc3BvbnNpYmxl
LWRpc2Nsb3N1cmVAc2lzYWwuaXQ+iJkEExYKAEEWIQSN1ZQWgDqtu8Ebq3f19kzv
K5YkKAUCYzMR+QIbAwUJA8NwJwULCQgHAgIiAgYVCgkICwIEFgIDAQIeBwIXgAAK
CRD19kzvK5YkKKrCAP9xe5WvRMRot7njmiwFWaYUyVVUcJYaePOKfGJ8B8w8UgEA
jfDw3QwZoZ5vV/iIDTu7IumcN8Vz4xHS5wtUq5Q8SAm4OARjMxH5EgorBgEEAZdV
AQUBAQdA9GpvoOxsD191XHuXU7sQNVqcjHyE9D03Ho6ccQExhiEDAQgHiH4EGBYK
ACYWIQSN1ZQWgDqtu8Ebq3f19kzvK5YkKAUCYzMR+QIbDAUJA8NwJwAKCRD19kzv
K5YkKOL3AP0avUZnHWfYjAJKkSuy4NkD0jpjrlewnyyByaWRTAHPugEA2YQj0P3J
s4shnxN+PxEapbs2WjvMdXSQtkie3XqNpA4=
=0qO1
-----END PGP PUBLIC KEY BLOCK-----

SISAL demande de fournir les informations suivantes :

- type de vulnérabilité ;
- service ou URL ou IP concerné(e) ;
- conditions et informations nécessaires pour reproduire le problème ;
- date à laquelle la vulnérabilité a été identifiée ;

- preuves relatives aux activités menées (par ex., POC) aux formats suivants : jpg, pdf, txt, vidéo. Les formats Word et Excel ne sont pas acceptés.

1.2 Types de vulnérabilité (exemples)

Les vulnérabilités énumérées ci-dessous relèvent de notre programme de sécurité.
Il est probable que tout problème de conception ou de mise en œuvre influençant de manière substantielle la confidentialité ou l'intégrité des données de l'utilisateur relève du domaine du programme. Les exemples courants incluent :

- Scripts intersites (XSS) ;
- Falsification de requête intersites (CSRF) ;
- Failles d'authentification ou d'autorisation ;
- Falsification de requête côté serveur (SSRF) ;
- Injection de template côté serveur (SSTI) ;
- Injection SQL (SQLI) ;
- Entité externe XML (XXE) ;
- Exécution de code à distance (RCE) ;
- Inclusions de fichier à distance ou localement.

1.3 Éléments non considérés comme des vulnérabilités :

- Spam par e-mail/SMS ou techniques d'ingénierie sociale ;
- Attaque DoS ou DDoS ;
- Injection de contenu. La publication de contenus sur un portail est une fonction fondamentale, par conséquent, l'injection de contenu (également connue comme « content spoofing » ou « injection HTML ») ne relève pas du domaine d'application, à moins qu'il existe la preuve manifeste d'un risque évident ;
- Signalisations d'interruptions soudaines sur une application mobile illisibles sur des versions mises à jour du système opérationnel ou sur des dispositifs mobiles publiés dans les 24 derniers mois.

1.4 Lignes directrices pour les chercheurs en sécurité

Sisal demande à tous les chercheurs en sécurité de suivre attentivement les lignes directrices suivantes et d'intervenir conformément aux normes en vigueur et applicables afin de ne pas commettre une infraction ou des délits informatiques potentiels punis par la loi (également par de l'emprisonnement) et donc, à titre indicatif et non exhaustif :

- De ne pas profiter de la vulnérabilité ou du problème découvert ;
- De ne pas mener des activités qui puissent :
  - nuire à Sisal ou à ses utilisateurs ;
  - bloquer un système ou un service de Sisal ;
  - entraîner la perte de données.

- De maintenir la confidentialité de toutes les informations relatives aux vulnérabilités découvertes jusqu'à 90 jours calendaires après qu'elles ont été notifiées à Sisal, sauf accord réciproque contraire ;

En faveur du respect de ces règles, Sisal s'engage à :

- Effectuer une première réponse de prise en charge de la signalisation en quelques jours ouvrables (généralement 7) ;
- Ne pas entreprendre d'actions en justice à l'encontre des chercheurs de sécurité qui signalent une vulnérabilité en suivant la présente politique ;
- Ne pas transmettre les données à caractère personnel à des tiers, sauf en cas d'obligations légales ;
- Informer les chercheurs au sujet des progrès et de la résolution des vulnérabilités détectées ;
- Ne pas offrir de récompense pour la signalisation d'une vulnérabilité.

Par ailleurs, Sisal **n'autorise pas** :

- L'insertion backdoor dans ses propres systèmes et applications ;
- L'ajout de modifications dans ses propres systèmes et applications ;
- La réalisation d'attaques DoS, DDoS, volumétriques ou par force brute ;
- La réalisation d'analyses automatisées surtout de manière agressive ;
- L'utilisation de l'ingénierie sociale sur des employés, des collaborateurs ou des exploitants.

Sisal se réserve, par ailleurs, le droit de mettre à jour la présente Politique de divulgation responsable à tout moment.