1 POLITICA DI DIVULGAZIONE RESPONSABILE

Sisal S.p.A. (di seguito Sisal) si adopera affinché il suo sistema di gestione per la sicurezza delle informazioni sia conforme a quanto previsto dagli standard ISO/IEC 27001 e WLA SCS-2020. Sisal chiede a tutti i ricercatori di sicurezza un contributo nel segnalare eventuali vulnerabilità che questi ultimi abbiamo potuto rilevare su prodotti o servizi Sisal al fine di proteggere al meglio gli utenti ed i loro dati.
Tutti i ricercatori di sicurezza potranno conoscere attraverso questa politica le modalità di segnalazione delle vulnerabilità.

1.1 Segnalazione vulnerabilità

Per segnalare a Sisal una vulnerabilità è possibile inviare un email a:
responsible-disclosure@sisal.it

Al fine di garantirne la confidenzialità delle informazioni, si richiede di cifrare il contenuto dell'email con l'apposita chiave PGP:

-----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 richiede di fornire le seguenti informazioni:

- tipo di vulnerabilità;
- servizio o URL o IP interessati;
- requisiti ed informazioni necessarie per riprodurre il problema;

- data in cui la vulnerabilità è stata identificata;
- evidenze relative alle attività svolte (es. poc) nei seguenti formati: jpg, pdf, txt, video. Non sono accettati formati quali word ed excel.

1.2 Tipologie di vulnerabilità (esempi)

Le vulnerabilità elencate in seguito sono idonee per il nostro programma di sicurezza.
È probabile che qualsiasi problema di progettazione o implementazione che influisca in modo sostanziale sulla riservatezza o l'integrità dei dati dell'utente rientri nell'ambito del programma. Esempi comuni includono:

- Cross-Site Scripting (XSS);
- Cross-Site Request Forgery (CSRF);
- Authentication or Authorization Flaws;
- Server-Side Request Forgery (SSRF);
- Server-Side Template Injection (SSTI);
- SQL injection (SQLI);
- XML External Entity (XXE);
- Remote Code Execution (RCE);
- Local or Remote File Inclusions.

1.3 Elementi non considerati vulnerabilità:

- Email/SMS Spam o tecniche di social engineering;
- DoS or DDoS attack;
- Content injection. La pubblicazione di contenuti su un portale è una funzione fondamentale, pertanto la content injection (nota anche come "content spoofing" o "HTML injection") non rientra nell'ambito di applicazione, a meno che non sia dimostrato chiaramente un evidente rischio;
- Segnalazioni di interruzioni improvvise su app mobile non riproducibili su versioni aggiornate del sistema operativo o su dispositivi mobili rilasciati negli ultimi 24 mesi.

1.4 Linee guida per i ricercatori di sicurezza

Sisal chiede a tutti i ricercatori di seguire con attenzione le seguenti linee guida e di operare in conformità alle normative vigenti e applicabili per non incorrere in violazioni o possibili reati informatici sanzionati dall'ordinamento giuridico (anche con la detenzione) e quindi a titolo esemplificativo e non esaustivo:

- Non sfruttare la vulnerabilità o la problematica scoperta;
- Non eseguire alcuna attività che possa:
  - danneggiare Sisal o i suoi utenti;
  - bloccare un sistema o un servizio di Sisal;
  - causare la perdita di dati.

- Mantenere riservate tutte le informazioni sulle vulnerabilità scoperte fino a 90 giorni di calendario dopo la notifica a Sisal, salvo diverso accordo reciproco;

Sisal a fronte del rispetto di queste regole si impegna a:

- Effettuare una prima risposta di presa in carico della segnalazione entro pochi giorni lavorativi (tipicamente 7);
- Non intraprendere alcuna azione legale nei confronti dei ricercatori di sicurezza che segnalano vulnerabilità seguendo questa policy;
- Non trasmettere i dati personali a terzi a meno di adempimenti di natura legale;
- Informare i ricercatori circa i progressi e la risoluzione delle vulnerabilità rilevate;
- Non offrire nessuna ricompensa per la segnalazione di vulnerabilità.

Inoltre, Sisal **non consente** di:

- Inserire backdoor nei propri sistemi ed applicazioni;
- Apportare modifiche ai propri sistemi e applicazioni;
- Effettuare attacchi DoS, DDoS, Volumetrici o Brute Force;
- Effettuare scansione automatizzate soprattutto in modalità aggressiva;
- Utilizzare l'ingegneria sociale su dipendenti, collaboratori ed esercenti.

Sisal si riserva inoltre il diritto di aggiornare la presente Politica di divulgazione responsabile in qualsiasi momento.