Vulnerability and Incident Disclosure Policy

Revision	*Author*	*Date*	*Notes*
1.0	Giuseppe Assalve	27 lug 2026	First Release

S.A.E.T. Srl | Via Busca, 61 | 12024 Costigliole Saluzzo (CN)
T. +39 0171 943959 | F. +39 0171 944831 | info@saetsrl.com
www.saetsrl.com| P.IVA 02165010048| REA CN-158505

Introduction

Since security is of critical importance to us and to our customers, we at SAET are committed to ensuring the safety and security of our products and services. SAET supports coordinated vulnerability disclosure and encourages responsible vulnerability testing, we take any reports of security issues seriously.
To report a potential security issue, please follow the steps described in the “Reporting procedure” section.

Reporting procedure

- Submit the Security Report at *security@saetsrl.com*
- Use our PGP public key (https://www.saetsrl.com/chi-siamo/certificazioni-e-standard/) to encrypt any email submissions.
- Write the Security Report in English or in Italian.
- Provide sufficient contact information, such as:
    a. your email;
    b. name of the person who found the security issue.
- Specify whether you are reporting:
    a. a potential vulnerability for which exploitation is not suspected, or
    b. a security incident or suspected active exploitation
- Provide the following information:
    a. date when the vulnerability or incident has been detected;
    b. details about how it has been discovered;
    c. a technical description of the issue.
- Provide as much information as you can on the product or service affected, such as:
    a. version number (hardware and software);
    b. configuration of the setup used.
- If you wrote specific proof-of-concept or exploit code of the vulnerability, please provide a copy. Please ensure all submitted code is clearly marked as such and is encrypted with our PGP key.
- If you have identified specific threats related to the root cause of the vulnerability or the incident, assessed the risk, or have seen the vulnerability being exploited in other products, please provide that information.

Internal assessment and action

1. SAET will acknowledge receiving your Security Report within *5* business days
    - If the Security Report contains all the required information, SAET will provide a unique tracking number and a contact person;
    - If the Security Report is not complete (more information is needed), SAET will request the missing information, and no more action will be taken.
2. SAET will start an internal management process to manage the reported security issue:
    - Receipt;
    - Triage;
    - Verification;
    - Remediation.
3. SAET will monitor the status of the management process, and you will receive a communication at the end of each stage.
4. SAET will use existing customer notification processes to manage the release of patches or security fixes, which may include without limitation and at SAET's sole discretion, direct customer notification or public release of an advisory notification on our website.
5. If the vulnerability or the incident source is actually in a third party component or service which is part of our product/service, SAET will notify the Security Report to that third party and advise you of that notification. To that end, please inform us in your email whether it is permissible in such cases to provide your contact information to the third party.

Notice

If you share any information with SAET in the context of responsible disclosure, you are agreeing that the information you submit will be considered as non-proprietary and non-confidential.
SAET is allowed to use shared information, or part of it, without any restriction. You agree that submitting information does not create any rights for you or any obligation for SAET.
Personal data is processed by SAET based on the privacy policy (https://www.saetsrl.com/chi-siamo/certificazioni-e-standard/).

Politica di divulgazione delle vulnerabilità e degli incidenti

Revision	*Author*	*Date*	*Notes*
1.0	Giuseppe Assalve	27 lug 2026	Primo rilascio

S.A.E.T. Srl | Via Busca, 61 | 12024 Costigliole Saluzzo (CN)
T. +39 0171 943959 | F. +39 0171 944831 | info@saetsrl.com
www.saetsrl.com| P.IVA 02165010048| REA CN-158505

Introduzione

Poiché la sicurezza è di fondamentale importanza per noi e per i nostri clienti, noi di SAET ci impegniamo a garantirla nei nostri prodotti e servizi. SAET sostiene la divulgazione coordinata delle vulnerabilità e incoraggia test responsabili; prendiamo molto sul serio qualsiasi segnalazione relativa a problemi in questo ambito.
Per segnalare un potenziale problema di sicurezza, si prega di seguire le indicazioni riportate nella sezione "Procedura di segnalazione".

Procedura di segnalazione

- Inviare il report di sicurezza all'indirizzo *security@saetsrl.com*
- Utilizzare la nostra chiave pubblica PGP (https://www.saetsrl.com/chi-siamo/certificazioni-e-standard/) per crittografare le comunicazioni via e-mail.
- Redigere il report di sicurezza in inglese o in italiano.
- Fornire informazioni di contatto sufficienti, quali:
    a. il proprio indirizzo e-mail;
    b. il nome della persona che ha individuato il problema di sicurezza.
- Specificare se si sta segnalando:
    a. una potenziale vulnerabilità per la quale non si sospetta un tentativo di sfruttamento, oppure
    b. un incidente di sicurezza o un sospetto sfruttamento attivo.
- Fornire le seguenti informazioni:
    a. data di rilevamento della vulnerabilità o dell'incidente;
    b. dettagli sulle modalità di scoperta;
    c. descrizione tecnica del problema.
- Fornire quante più informazioni possibili sul prodotto o servizio interessato, quali:
    a. numero di versione (hardware e software);
    b. configurazione del sistema utilizzato.
- Se è stato realizzato un proof-of-concept o un codice exploit specifico per la vulnerabilità, si prega di fornirne una copia. Assicurarsi che tutto il codice inviato sia chiaramente identificato come tale e crittografato con la nostra chiave PGP.
- Se sono state individuate minacce specifiche correlate alla causa scatenante della vulnerabilità o dell'incidente, se è stata effettuata una valutazione del rischio o se si è osservato lo sfruttamento della vulnerabilità in altri prodotti, si prega di fornire tali informazioni.

Valutazione ed azioni interne

6. SAET confermerà la ricezione della vostra segnalazione di sicurezza entro 5 giorni lavorativi:
    - Se la segnalazione contiene tutte le informazioni richieste, SAET fornirà un numero di riferimento univoco e un referente;
    - Se la segnalazione non è completa (sono necessarie ulteriori informazioni), SAET richiederà le informazioni mancanti e non intraprenderà ulteriori azioni.
7. SAET avvierà un processo interno per gestire la problematica di sicurezza segnalata:
    - Ricezione;
    - Triage;
    - Verifica;
    - Risoluzione.
8. SAET monitorerà lo stato del processo di gestione e riceverete una comunicazione al termine di ogni fase.
9. SAET utilizzerà le procedure esistenti di notifica ai clienti per gestire il rilascio di patch o correzioni di sicurezza; tali procedure possono includere, a titolo esemplificativo e a esclusiva discrezione di SAET, la notifica diretta al cliente o la pubblicazione di un avviso di sicurezza sul nostro sito web.
10. Qualora la vulnerabilità o la causa dell'incidente riguardino effettivamente un componente o un servizio di terze parti integrato nel nostro prodotto/servizio, SAET inoltrerà la segnalazione di sicurezza alla terza parte interessata e vi informerà di tale inoltro. A tal fine, vi preghiamo di indicare nell'e-mail se, in tali casi, sia consentito fornire i vostri recapiti alla terza parte.

Avviso

Condividendo informazioni con SAET nell'ambito della divulgazione responsabile, si accetta che le informazioni trasmesse siano considerate non proprietarie e non riservate. SAET è autorizzata a utilizzare le informazioni condivise, o parte di esse, senza alcuna restrizione. Si accetta che l'invio di informazioni non conferisce alcun diritto né crea alcun obbligo in capo a SAET.
I dati personali sono trattati da SAET in conformità con l'informativa sulla privacy. (https://www.saetsrl.com/chi-siamo/certificazioni-e-standard/).

S.A.E.T. Srl | Via Busca, 61 | 12024 Costigliole Saluzzo (CN)
T. +39 0171 943959 | F. +39 0171 944831 | info@saetsrl.com
www.saetsrl.com| P.IVA 02165010048| REA CN-158505