Politica per la segnalazione coordinata delle vulnerabilità

1. Scopo

Gasparini S.p.A. considera la segnalazione responsabile delle vulnerabilità una parte essenziale del processo di sicurezza informatica dei propri prodotti.

Questa policy descrive come clienti, ricercatori di sicurezza informatica, partner, fornitori e altri soggetti possono comunicare a Gasparini S.p.A. una potenziale vulnerabilità, quali informazioni sono utili per consentirne l'analisi e come viene gestito il successivo coordinamento.

L'obiettivo è permettere a Gasparini S.p.A. di verificare il problema, identificare i prodotti e le versioni interessate e predisporre eventuali misure correttive o di mitigazione prima che informazioni tecniche dettagliate vengano rese pubbliche.

La policy costituisce il punto di riferimento pubblico per la segnalazione delle vulnerabilità relative ai prodotti Gasparini S.p.A..

2. Ambito di applicazione

Possono essere segnalate attraverso questa procedura vulnerabilità o debolezze di sicurezza informatica che interessano prodotti Gasparini S.p.A. contenenti componenti digitali, inclusi, quando applicabile:

- software applicativo;
- software HMI;
- firmware;
- sistemi operativi e relative configurazioni quando forniti come parte della macchina;
- servizi e componenti software sviluppati da Gasparini S.p.A.;
- librerie e componenti software di terze parti integrati nel prodotto;
- interfacce di rete, protocolli e servizi esposti dal prodotto;
- meccanismi di autenticazione e autorizzazione;
- funzionalità di aggiornamento o manutenzione remota;
- configurazioni che possono avere un impatto sulla sicurezza del prodotto.

Una vulnerabilità relativa a un componente di terze parti può essere segnalata a Gasparini S.p.A. quando tale componente è utilizzato all'interno di un prodotto Gasparini S.p.A.. In questi casi Gasparini S.p.A. valuterà l'impatto sui propri prodotti e, quando necessario, coordinerà la gestione del problema con il produttore o manutentore del componente.

Richieste di assistenza tecnica che non riguardano un problema di sicurezza informatica devono invece essere indirizzate ai normali canali di supporto Gasparini S.p.A..

3. Come segnalare una vulnerabilità

Le vulnerabilità possono essere segnalate attraverso il seguente punto di contatto:

Pagina web: https://www.gasparini-spa.com/service/sicurezza-informatica/

Il punto di contatto indicato deve essere utilizzato esclusivamente o prevalentemente per questioni relative alla sicurezza informatica dei prodotti, in modo da consentire una presa in carico tempestiva da parte del personale incaricato.

Per informazioni tecniche particolarmente sensibili sarà disponibile un canale di comunicazione protetto:

e-mail con cifratura PGP

La pagina web dedicata alla segnalazione dovrà rendere disponibili sia questa policy sia le informazioni necessarie per utilizzare il canale sicuro.

4. Informazioni da includere nella segnalazione

Una segnalazione dovrebbe però contenere informazioni sufficienti per permettere a Gasparini S.p.A. di comprendere il problema e iniziare l'analisi.

Quando disponibili, è utile indicare:

- numero di matricola
- descrizione della vulnerabilità
- componente nel quale è stato individuato il problema
- condizioni necessarie per riprodurre la vulnerabilità
- passaggi utilizzati per verificare la vulnerabilità
- possibile impatto sulla sicurezza del macchinario e/o dell’operatore
- eventuale codice dimostrativo, log, screenshot o altre evidenze tecniche (in forma di file allegati)
- informazioni sull'eventuale conoscenza pubblica o sfruttamento della vulnerabilità
- Informazioni di contatto (indirizzo e-mail)

Il segnalante dovrebbe fornire anche un recapito che consenta a Gasparini S.p.A. di chiedere chiarimenti durante l'analisi.

Non è necessario trasmettere dati personali, credenziali, informazioni riservate di clienti o altri dati che non siano strettamente necessari a dimostrare la vulnerabilità.

5. Gestione della segnalazione

Gasparini S.p.A. registra le segnalazioni ricevute e ne effettua una prima valutazione per determinare se il problema descritto riguarda un prodotto nel proprio perimetro e se le informazioni disponibili sono sufficienti per procedere con l'analisi.

Quando il segnalante ha fornito un recapito valido, Gasparini S.p.A. conferma la ricezione della segnalazione e può richiedere ulteriori informazioni o evidenze tecniche.

La successiva analisi può comprendere la riproduzione del problema, l'identificazione delle versioni e dei componenti interessati, la valutazione dell'impatto e la definizione delle possibili misure correttive.

Quando la vulnerabilità riguarda un componente sviluppato o mantenuto da una terza parte, Gasparini S.p.A. può coinvolgere il relativo produttore, fornitore o maintainer, limitando le informazioni condivise a quelle necessarie per analizzare e risolvere il problema.

I tempi necessari per l'analisi e la correzione dipendono dalla natura della vulnerabilità, dalla sua complessità, dai prodotti interessati e dalla disponibilità di una misura di mitigazione o di un aggiornamento.

Gasparini S.p.A. mantiene, per quanto possibile, il contatto con il segnalante durante le principali fasi di gestione del caso.

6. Gestione coordinata della divulgazione

Gasparini S.p.A. chiede a chi segnala una vulnerabilità di non pubblicare dettagli tecnici che possano facilitarne lo sfruttamento prima che il problema sia stato analizzato e sia stato possibile predisporre una misura correttiva o di mitigazione.

Quando è prevista una divulgazione pubblica, Gasparini S.p.A. e il segnalante possono concordare tempi e modalità della pubblicazione considerando:

- gravità della vulnerabilità;
- probabilità e facilità di sfruttamento;
- eventuale presenza di sfruttamento attivo;
- disponibilità di workaround;
- disponibilità di un aggiornamento di sicurezza informatica;
- tempo ragionevolmente necessario agli utilizzatori per applicare la correzione;
- eventuale coinvolgimento di altri produttori o componenti vulnerabili.

La richiesta di coordinamento non ha lo scopo di impedire la divulgazione di una vulnerabilità, ma di ridurre il rischio per gli utilizzatori durante il periodo necessario alla sua analisi e correzione.

Quando viene pubblicato un aggiornamento di sicurezza informatica, Gasparini S.p.A. può rendere disponibili informazioni che consentano agli utilizzatori di identificare il prodotto interessato, comprendere l'impatto della vulnerabilità e adottare le misure necessarie.

7. Comportamento richiesto durante le attività di ricerca

Gasparini S.p.A. chiede a chi svolge attività di ricerca sulla sicurezza informatica dei propri prodotti di operare in modo proporzionato rispetto alla necessità di verificare l'esistenza della vulnerabilità.

In particolare, la verifica non dovrebbe comportare:

- accesso intenzionale a dati personali o informazioni riservate non necessarie alla ricerca;
- modifica o cancellazione di dati;
- alterazione permanente della configurazione del prodotto;
- interruzione deliberata di servizi o processi produttivi;
- compromissione di sistemi appartenenti a clienti o terze parti;
- installazione di meccanismi di persistenza;
- utilizzo della vulnerabilità per ottenere un accesso ulteriore rispetto a quanto necessario per dimostrarne l'esistenza;
- attività che possano compromettere la sicurezza fisica di persone, macchinari o impianti.

Se durante la verifica vengono accidentalmente individuati dati personali, credenziali o altre informazioni riservate, l'attività dovrebbe essere interrotta una volta raccolti gli elementi minimi necessari a dimostrare il problema. Tali informazioni non dovrebbero essere conservate, utilizzate o diffuse oltre quanto strettamente necessario per la segnalazione.

Particolare cautela deve essere adottata sulle macchine industriali operative. Una verifica di sicurezza informatica non deve introdurre rischi per persone, impianti, produzione o ambiente.

8. Vulnerabilità già note o relative a componenti di terze parti

La presenza di una vulnerabilità pubblicamente nota in un componente utilizzato da un prodotto Gasparini S.p.A. non implica automaticamente che il prodotto sia vulnerabile.

La segnalazione dovrebbe, quando possibile, indicare perché la vulnerabilità è ritenuta applicabile al prodotto Gasparini S.p.A., specificando il componente e la versione interessati.

Gasparini S.p.A. valuterà l'effettiva esposizione del prodotto e le condizioni necessarie per lo sfruttamento.

Nel caso di vulnerabilità originata da un componente di terze parti, la gestione potrà richiedere il coordinamento con il relativo fornitore prima che possa essere resa disponibile una correzione.

9. Comunicazioni e riconoscimento del segnalante

Quando appropriato e previo consenso, Gasparini S.p.A. può riconoscere pubblicamente il contributo del ricercatore o del soggetto che ha segnalato la vulnerabilità.

La decisione di citare il segnalante viene concordata prima della pubblicazione di eventuali security advisory o altre comunicazioni pubbliche.

La presente policy non costituisce un programma di bug bounty e non prevede automaticamente premi o compensi economici per le vulnerabilità segnalate.

10. Segnalazioni incomplete, non pertinenti o non verificabili

Gasparini S.p.A. può chiudere una segnalazione quando:

- il problema non riguarda un prodotto Gasparini S.p.A.;
- non è possibile ottenere informazioni sufficienti per comprenderlo o riprodurlo;
- il comportamento segnalato non costituisce una vulnerabilità di sicurezza informatica;
- il problema è già noto ed è già in gestione;
- la segnalazione riguarda esclusivamente una richiesta di assistenza tecnica.

Quando possibile, la motivazione della chiusura viene comunicata al segnalante.

Una segnalazione chiusa può essere rivalutata se vengono successivamente fornite nuove evidenze tecniche.

11. Vulnerabilità con impatto elevato o sfruttamento attivo

Una segnalazione che indichi un possibile sfruttamento attivo, una compromissione già avvenuta o un impatto significativo sulla sicurezza del prodotto (safety) viene trattata con priorità.

Gasparini S.p.A. può richiedere rapidamente ulteriori informazioni al segnalante e attivare le proprie procedure interne di escalation, gestione delle vulnerabilità e, quando applicabile, gli adempimenti previsti dalla normativa vigente.

Il processo di segnalazione previsto da questa policy è distinto dagli eventuali obblighi normativi di comunicazione verso le autorità competenti, che vengono gestiti internamente da Gasparini S.p.A..

12. Protezione delle informazioni ricevute

Le informazioni relative a vulnerabilità non ancora corrette devono essere trattate con particolare cautela.

Gasparini S.p.A. limita l'accesso ai dettagli tecnici alle persone che necessitano di tali informazioni per analizzare il problema, sviluppare una correzione, coordinarsi con eventuali soggetti coinvolti o adempiere a obblighi normativi.

Quando la gestione della vulnerabilità richiede il coinvolgimento di fornitori, partner o altri produttori, vengono condivise le sole informazioni necessarie per la gestione del problema.

13. Aggiornamento della policy

Questa policy viene riesaminata quando cambiano i canali di segnalazione, il processo interno di gestione delle vulnerabilità o i requisiti normativi applicabili.

La versione corrente deve essere disponibile sul sito web Gasparini S.p.A. insieme al punto di contatto utilizzato per le segnalazioni.

Riferimenti

La policy è stata impostata tenendo conto dei requisiti di vulnerability handling del **Regolamento (UE) 2024/2847, Cyber Resilience Act**. L'Annex I, Part II richiede ai produttori di adottare e applicare una coordinated vulnerability disclosure policy e di facilitare la condivisione delle informazioni sulle vulnerabilità, mettendo a disposizione un indirizzo per le segnalazioni. L'Annex II richiede inoltre che le informazioni fornite con il prodotto indichino il punto unico di contatto presso il quale possono essere segnalate le vulnerabilità e reperita la relativa policy.

Come riferimento tecnico è stato considerato anche il **prEN 40000-1-3:2025, Vulnerability Handling Requirements**, in particolare per gli aspetti relativi alla CVD policy, alla comunicazione sicura e alla capacità di ricevere e gestire le segnalazioni. Alla data di redazione il documento è ancora un progetto di norma e non è citato nella Gazzetta ufficiale dell'Unione europea, pertanto non conferisce ancora presunzione di conformità al CRA.

Stato: Approvato [sb]
Versione: 0.3 [sb]
Organizzazione: Gasparini S.p.A.
Classificazione: Pubblico