Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO P07



VERSIONE 2.0 · DICEMBRE 2026

Politica di gestione delle vulnerabilità

Come Trailgun scopre, valuta e corregge le vulnerabilità, con quali tempi, come le comunica ai Clienti e come accoglie le segnalazioni di chi le trova.

CODICE	TITOLARE	REVISIONE	STATO
P07 · POL-07	Responsabile della sicurezza	Annuale	al 01/12/2026

POLITICA P07 · POL-07

Politica di gestione delle vulnerabilità

Come Trailgun scopre, valuta e corregge le vulnerabilità, con quali tempi, e come le comunica.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P07 (POL-07)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	personale tecnico; uffici ICT risk e CISO dei Clienti; ricercatori di sicurezza	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P05, P06, P08; procedura 24 (Gestione delle vulnerabilità e segnalazione responsabile); procedura 25 (Risposta agli incidenti); documento 12 (Percorso di certificazione e piattaforma)

AMBITO

Componenti in uso nella piattaforma: codice, dipendenze, immagini dei container, sistema operativo dell'host, proxy Caddy, servizi AWS configurati da Trailgun.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
8.8, 5.7, 6.8	DORA artt. 9(4)(f), 25; Reg. del. (UE) 2024/1774 art. 10

1 Scopo e ruoli

Una vulnerabilità nota e non corretta è il modo più comune in cui un servizio viene violato. Il Responsabile della sicurezza valuta ogni vulnerabilità, ne decide la gravità e il trattamento e verifica che i tempi del § 3 siano rispettati; chi sviluppa prepara la correzione con un cambiamento ordinario o urgente (politica P05).

2 Fonti

- Dependabot, settimanale, su tutte le dipendenze; scansione di ogni immagine al caricamento nel registro delle immagini.
- Scansione dei segreti (gitleaks) sull'intera storia del repository a ogni verifica della CI.
- Bollettini dei fornitori (AWS, Node.js, Caddy, LibreOffice, Chromium) e catalogo CISA delle vulnerabilità sfruttate (KEV).
- Segnalazioni esterne a security@trailgun.ai, secondo la politica di segnalazione responsabile pubblicata su https://trailgun.ai/security e in https://trailgun.ai/.well-known/security.txt (procedura 24); segnalazioni dei Clienti.
- Prove indipendenti: scansione esterna mensile dell'applicazione e penetration test annuale (Percorso, tappe R05 e R06).

3 Valutazione e tempi di correzione

La gravità si misura con CVSS v3.1 o v4. I tempi decorrono dalla disponibilità della correzione, per vulnerabilità che toccano componenti in uso. Se la correzione non c'è, si adotta subito una mitigazione (configurazione, disattivazione della funzione, regola di rete) e la si registra.

GRAVITÀ	CRITERIO	TEMPO MASSIMO	NOTE
Critica	CVSS ≥ 9,0 o sfruttata attivamente (KEV)	72 ore	mitigazione immediata se manca la correzione; valutazione come minaccia per i Clienti
Alta	CVSS 7,0-8,9	7 giorni	
Media	CVSS 4,0-6,9	30 giorni	
Bassa	CVSS < 4,0	90 giorni	
Sistema dell'host	aggiornamenti di sicurezza dell'immagine del sistema operativo	ogni mese	e subito, come critica, per una vulnerabilità critica del sistema

4 Il trattamento di una vulnerabilità

1. **Ricezione.** Ogni segnalazione o avviso si apre come voce di lavoro con fonte, componente e data di disponibilità della correzione.
2. **Valutazione.** Il Responsabile della sicurezza conferma se il componente è in uso e raggiungibile, assegna la gravità e il termine del § 3.

3 **Correzione o mitigazione.** Aggiornamento con un cambiamento ordinario o, per le critiche, urgente (politica P05); se la correzione manca, mitigazione registrata.

4 **Verifica.** La verifica della CI e la nuova scansione dell'immagine confermano la chiusura.

5 **Comunicazione.** Ai Clienti secondo il § 5; al segnalatore secondo la procedura 24.

5 Comunicazione

5.1 Una vulnerabilità che può riguardare un Cliente si tratta come minaccia informatica significativa e gli si comunica entro 24 ore; se è stata sfruttata, è un incidente (procedura 25).

5.2 Il rispetto dei tempi di correzione è nel rapporto di servizio (Percorso, tappa R04) e si comunica al Cliente che lo chiede; al Cliente si consegna, sotto riservatezza, la sintesi dei risultati del penetration test e il piano di rimedio.

5.3 Trailgun partecipa, alle condizioni concordate per non mettere a rischio gli altri clienti, ai test guidati dalla minaccia (TLPT) dei Clienti DORA (art. 26 DORA).

6 Segnalazione responsabile

Chi trova una vulnerabilità scrive a security@trailgun.ai. Trailgun conferma la ricezione, valuta e comunica l'esito, e non agisce contro chi segnala in buona fede senza accedere ai dati di altri, senza degradare il servizio e senza divulgare prima della correzione. Ambito, regole e tempi di risposta sono nella procedura 24, che riporta anche il testo pubblicato di security.txt.

7 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Dependabot e scansione delle immagini	IN ESSERE avvisi e richieste di aggiornamento	settimanale; a ogni immagine
Tempi di correzione	IN ESSERE data di apertura, gravità, termine e chiusura di ogni voce	registro dei cambiamenti (45)
Aggiornamento mensile del sistema	IN ESSERE nuova immagine del sistema operativo ogni mese	registro dei cambiamenti
Segnalazione responsabile	IN ESSERE security.txt e pagina /security pubblicati	trailgun.ai; scadenza di security.txt rinnovata ogni anno

8 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8: una correzione rinviata oltre i tempi richiede una mitigazione registrata e, per le critiche e le alte, l'approvazione del Responsabile della sicurezza con una nuova data. Riferimenti: DORA art. 9, par. 4, lett. f), e artt. 25-26; Reg. del. (UE) 2024/1774 art. 10; ISO/IEC 27001:2022 controlli 5.7, 6.8 e 8.8; RFC 9116 (security.txt).