Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 24

VERSIONE 2.0 · DICEMBRE 2026

Procedura di gestione delle vulnerabilità e di segnalazione responsabile

Da dove arrivano le vulnerabilità, come si valutano e in quanto tempo si correggono; e la politica di segnalazione responsabile per chi ne trova una, con il testo integrale di security.txt. La parte 2 è il testo pubblicato su https://trailgun.ai/security.

CRITICA	ALTA	MEDIA	BASSA
72 ore	7 giorni	30 giorni	90 giorni

PROCEDURA 24 · PROC-24

Gestione delle vulnerabilità e segnalazione responsabile

Parte 1: come Trailgun scopre, valuta, corregge e comunica le vulnerabilità. Parte 2: come segnalarne una a Trailgun, e che cosa Trailgun si impegna a fare.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
PROC-24	Responsabile della sicurezza (Franco Puppo, CEO)	Organo amministrativo, [data della delibera]	2.0 · stato al 01/12/2026

REVISIONE	DESTINATARI
annuale, con il rinnovo di security.txt	chi sviluppa e amministra la piattaforma; CISO dei Clienti; ricercatori di sicurezza (parte 2)

DOCUMENTI COLLEGATI

politica P07; documento 20, Gestione dei cambiamenti; documento 23, Chiavi e segreti; documento 25, Risposta agli incidenti; documento 41, Registro dei rischi ICT; documento 12, Percorso di certificazione e piattaforma

PARTE 1

Gestione delle vulnerabilità

1 Scopo e ambito

Ogni componente in uso nella piattaforma: codice di Trailgun, dipendenze, immagini dei container (Node.js, LibreOffice, Chromium, Caddy), sistema operativo dell'host, configurazione dei servizi AWS gestiti da Trailgun, sito e backoffice. Ruoli: il Responsabile della sicurezza valuta, decide i tempi e le eccezioni e tiene il registro; chi sviluppa corregge seguendo il documento 20.

2 Fonti

- **Dependabot**: avvisi di sicurezza e correzioni appena l'avviso è pubblicato; aggiornamenti settimanali di dipendenze, immagini di base e azioni dell'integrazione continua.
- **Scansione delle immagini** nel registro ECR a ogni caricamento.
- **Scansione dei segreti** (gitleaks) su tutta la storia del repository a ogni verifica (documento 23).
- **Bollettini** di AWS, Node.js, Caddy, LibreOffice e Chromium, e il catalogo CISA delle vulnerabilità sfruttate attivamente (KEV).
- **GuardDuty**, allarmi e log, quando un comportamento anomalo rivela una debolezza.
- **Segnalazioni** dei Clienti e dei ricercatori a security@trailgun.ai (parte 2).
- La scansione esterna mensile dell'applicazione e il penetration test indipendente annuale sono le tappe R05 e R06 del Percorso (documento 12); i loro risultati entreranno in questa procedura come ogni altra fonte.

3 Passi

1 **Registrare** la vulnerabilità con la fonte, il componente, la versione e la data in cui la correzione è disponibile: da lì decorrono i tempi.

2 **Valutare** se tocca un componente in uso e se è raggiungibile; assegnare la gravità con CVSS v3.1 o v4, alzandola se la vulnerabilità è sfruttata attivamente (KEV) o esposta su Internet.

3 **Correggere** nei tempi della tabella 4 con un cambiamento (documento 20), urgente per le critiche. Se la correzione non esiste, adottare subito una mitigazione (configurazione, disattivazione della funzione, regola di rete) e registrarla.

4 **Verificare** che la correzione sia in production (versione del componente nell'immagine pubblicata, nuova scansione) e chiudere la voce con la data.

5 **Comunicare**: 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 e segue il documento 25.

4 · GRAVITÀ	CRITERIO	TEMPO MASSIMO	NOTE
Critica	CVSS ≥ 9,0, o sfruttata attivamente (KEV)	72 ore	mitigazione immediata se manca la correzione
Alta	CVSS 7,0–8,9	7 giorni	

4 · GRAVITÀ	CRITERIO	TEMPO MASSIMO	NOTE
Media	CVSS 4,0-6,9	30 giorni	
Bassa	CVSS < 4,0	90 giorni	
Sistema dell'host	aggiornamenti di sicurezza dell'AMI	ogni mese	più le critiche nei tempi sopra

I tempi decorrono dalla disponibilità della correzione, per vulnerabilità che toccano componenti in uso. La gravità si misura con CVSS v3.1 o v4.

5 Eccezioni

Un tempo della tabella 4 si supera solo con un'eccezione scritta del Responsabile della sicurezza: motivo, mitigazione in essere, nuova data. L'eccezione entra nel registro dei rischi (documento 41) e scade alla nuova data. Nessuna eccezione per una vulnerabilità critica sfruttata attivamente senza una mitigazione efficace.

6 Evidenze e riferimenti

6.1 Evidenze: registro delle vulnerabilità con date e tempi; avvisi Dependabot e pull request collegate; risultati delle scansioni ECR e gitleaks; eccezioni nel registro dei rischi; versione dell'AMI in uso.

6.2 Riferimenti: DORA, art. 9, par. 4, lett. f); Reg. del. (UE) 2024/1774, art. 10 (gestione delle vulnerabilità e delle patch); ISO/IEC 27001:2022, controllo 8.8 (gestione delle vulnerabilità tecniche); RFC 9116 (security.txt).

PARTE 2 · TESTO PUBBLICATO SU HTTPS://TRAILGUN.AI/SECURITY

Politica di segnalazione responsabile

Se pensi di aver trovato una vulnerabilità in Trailgun, scrivici. Ti rispondiamo, la correggiamo e non agiamo contro di te se rispetti le regole qui sotto.

7 Come segnalare

Scrivi a **security@trailgun.ai**, in italiano o in inglese. Indica: la pagina, l'indirizzo o la funzione interessati; i passi per riprodurre il problema; l'impatto che hai osservato; data e ora delle prove; un recapito. Non mandare dati personali di terzi che avessi visto: descrivili. Se devi inviare materiale delicato, chiedi nella prima email un canale dedicato: ti mandiamo un link temporaneo cifrato.

8 Ambito

8.1 **Compreso**: i siti e i servizi di Trailgun su `trailgun.ai`, `www.trailgun.ai`, `app.trailgun.ai` (compresa l'API pubblica `/api/v1`) e `backoffice.trailgun.ai`; la ricezione delle email su `mail.trailgun.ai`.

8.2 **Escluso**: i servizi dei fornitori (per esempio AWS, i provider di posta e di pagamento), da segnalare a loro; attacchi di negazione del servizio o test di carico; ingegneria sociale verso persone di Trailgun o dei Clienti; accessi fisici; invio di spam; risultati di scanner automatici senza un impatto dimostrato.

9 Regole per chi segnala

- Usa solo account tuoi o account di prova; non accedere, modificare o cancellare dati di altri oltre il minimo indispensabile per dimostrare il problema, e fermati appena vedi dati di terzi.
- Non degradare il servizio e non usare la vulnerabilità oltre la prova.
- Non conservare né divulgare dati che hai visto; cancellali a fine segnalazione.
- Non rendere pubblica la vulnerabilità prima della correzione, e comunque non prima che siano trascorsi i tempi della tabella 4 per la sua gravità (al massimo 90 giorni dalla segnalazione), salvo un accordo diverso con noi.

10 Che cosa fa Trailgun

- Conferma la ricezione con una risposta automatica, subito, e ti risponde nel merito con una prima valutazione entro [n] giorni lavorativi.
- Corregge nei tempi della tabella 4 secondo la gravità e ti tiene aggiornato sullo stato.
- Ti comunica la correzione e, se lo desideri, ti ringrazia per nome nella comunicazione.
- Tratta come autorizzata, per le sole finalità della prova, la ricerca svolta in buona fede nel rispetto di queste regole: non presenta denunce o querele e non promuove azioni civili contro di te per quella ricerca. Se un terzo agisce contro di te per un'attività conforme a questa politica, Trailgun dichiara, a chi lo chiede, che quell'attività era autorizzata da questa politica.
- Il programma non prevede compensi in denaro.

11 Testo integrale di security.txt

Pubblicato su `https://trailgun.ai/.well-known/security.txt` secondo la RFC 9116 e servito solo in HTTPS; non è firmato con OpenPGP e Trailgun non pubblica una chiave PGP. Il campo `Expires` si rinnova a ogni revisione annuale, prima della scadenza, e non supera mai un anno.

```
Contact: mailto:security@trailgun.ai
Expires: 2027-11-30T23:59:59+01:00
Preferred-Languages: it, en
Canonical: https://trailgun.ai/.well-known/security.txt
Policy: https://trailgun.ai/security
```

Trailgun

On target.

In a flash.

Dai documenti al lavoro finito: agenti AI per pratiche legali e finanziarie.

SICUREZZA E INCIDENTI, 24/7
security@trailgun.ai

REPERIBILITÀ PRIORITÀ 1
[+39 ...]

PRIVACY E DPO
privacy@trailgun.ai

Procedura 24 del pacchetto di conformità Trailgun, versione 2.0, stato al 01/12/2026. Attua la politica P07 (gestione delle vulnerabilità). La parte 2 e il file security.txt sono pubblici: https://trailgun.ai/security e https://trailgun.ai/.well-known/security.txt.