

# Manutenzione programmata Kernel Linux - mitigazione sicurezza ptrace

Stato	<b>Completato</b>
Tipo	Manutenzione programmata
Pubblicato il	2026-05-23 08:45 UTC
Inizio finestra	2026-05-23 08:45 UTC
Fine finestra	2026-05-23 09:00 UTC
Completato il	2026-05-23 08:58 UTC

Informiamo i gentili clienti che verrà eseguita un'attività programmata di hardening sui sistemi Linux, a seguito della recente segnalazione relativa alla vulnerabilità **CVE-2026-46333**, associata a un possibile rischio di accesso non autorizzato tramite meccanismi legati a **ptrace** e alla funzione `__ptrace_may_access()` del Kernel Linux.

Specifichiamo che, già allo stato attuale, le vulnerabilità note del Kernel risultano **patchate o rese non sfruttabili** attraverso l'applicazione di misure di mitigazione mirate, tra cui la rimozione dei moduli coinvolti, la relativa blacklist degli stessi e, dove necessario, l'applicazione della policy restrittiva:

```
sysctl -w kernel.yama.ptrace_scope=3
```

Questa configurazione aumenta il livello di restrizione sull'utilizzo di **ptrace**, riducendo ulteriormente la superficie di attacco in attesa degli aggiornamenti kernel definitivi forniti dai vendor di riferimento.

A seguito dell'applicazione di questa policy, eventuali funzionalità di debug, tracing o diagnostica che fanno uso di **ptrace** potrebbero non funzionare correttamente o risultare non disponibili. L'impatto riguarda esclusivamente strumenti e procedure tecniche avanzate, mentre non sono previste ripercussioni sul normale funzionamento dei servizi web, database, posta o applicazioni ospitate.

Un aggiornamento completo del Kernel all'ultima versione disponibile del **ramo 7** verrà pianificato indicativamente per **metà giugno 2026**, come intervento cumulativo volto a recepire eventuali ulteriori correzioni che dovessero essere rilasciate nelle prossime settimane. Tale approccio consente di evitare interventi frammentati e potenzialmente più invasivi, come la rimozione di moduli o la disabilitazione di specifiche funzionalità, salvo diverse necessità di sicurezza.

Non sono previsti downtime, reboot o interruzioni del servizio durante questa attività.