

RICERCA CVEs UBUNTU 24.04 con ChatGPT

Prompt: *Informami dettagliatamente e precisamente su tutti i più importanti CVE di Ubuntu 24.04 che conosci .*

Risposta:

Ecco alcuni dei più importanti CVE che hanno interessato Ubuntu 24.04:

1. **CVE-2024-6387 (regreSSHion):** Una **vulnerabilità in OpenSSH** che gestiva in modo errato i segnali, permettendo a un attaccante remoto di bypassare l'autenticazione e accedere al sistema senza credenziali valide. [Ubuntu](#)
2. **CVE-2024-50264:** Una **vulnerabilità nel kernel** Linux relativa a un puntatore pendente in vsk->trans, che poteva portare a una condizione di Use-After-Free, consentendo a utenti locali di elevare i propri privilegi. [Ubuntu](#)
3. **CVE-2024-42009:** Una vulnerabilità di **Cross-Site Scripting (XSS) in Roundcube** fino alla versione 1.5.7 e 1.6.x fino alla 1.6.7, che permetteva a un attaccante remoto di rubare e inviare email della vittima tramite un messaggio email appositamente creato. [GitHub](#)
4. **CVE-2024-11694:** Una **vulnerabilità in Firefox** che poteva portare a potenziali esecuzioni di codice arbitrario o crash dell'applicazione. [Ubuntu](#)
5. **CVE-2024-0126:** Una **vulnerabilità nel driver NVIDIA GPU Display** per Windows e Linux che poteva permettere a un attaccante privilegiato di elevare i propri permessi, portando a esecuzione di codice, denial of service, divulgazione di informazioni e manomissione dei dati. [Ubuntu](#)
6. **CVE-2024-45490:** Una **vulnerabilità in libcue** che poteva portare a un buffer overflow, causando potenzialmente l'esecuzione di codice arbitrario. [Ubuntu](#)
7. **CVE-2024-45004:** Una **vulnerabilità nel kernel** Linux riguardante una perdita di chiave di crittografia nel sottosistema Trusted Keys, che poteva portare a una divulgazione non autorizzata di informazioni sensibili. [Ubuntu](#)

È fondamentale mantenere il sistema aggiornato per proteggersi da queste e altre vulnerabilità. Si consiglia di consultare regolarmente le Notifiche di Sicurezza di Ubuntu per informazioni aggiornate sulle vulnerabilità e le relative patch.

Prompt : Espandi dettagliatamente la n.1

Risposta :

La vulnerabilità **CVE-2024-6387**, denominata *regreSSHion*, è una falla critica individuata in OpenSSH, il software di riferimento per l'accesso remoto sicuro ai sistemi basati su Unix/Linux. Ecco i dettagli:

Descrizione del problema

La vulnerabilità riguarda un'errata gestione dei segnali all'interno del processo del demone SSH (*sshd*). Nello specifico, un errore nella logica di gestione del segnale SIGPIPE permetteva a un attaccante remoto di sfruttare un comportamento inatteso del sistema durante l'autenticazione, bypassando i meccanismi di sicurezza.

Come sfruttare la vulnerabilità

Un attaccante poteva sfruttare la vulnerabilità in questo modo:

1. Preparazione:

- L'attaccante doveva conoscere un nome utente valido sul sistema vulnerabile.
- Non erano necessarie credenziali valide, ma solo l'accesso alla porta SSH aperta (tipicamente la porta 22).

2. Invio di richieste manipolate:

- L'attaccante inviava un flusso di dati appositamente costruito al server SSH, progettato per causare una condizione di errore legata a SIGPIPE.
- Il bug si attivava durante una fase specifica del processo di autenticazione, creando una condizione di *race* (competizione tra processi).

3. Effetto del bug:

- A causa dell'errata gestione del segnale, OpenSSH interpretava erroneamente il fallimento dell'autenticazione come un successo.
- Questo permetteva all'attaccante di ottenere una sessione SSH completamente autenticata.

4. Accesso al sistema:

- L'attaccante otteneva accesso alla shell come il nome utente target (se il nome utente aveva privilegi amministrativi, l'attaccante poteva ottenere il controllo completo del sistema).

Impatto della vulnerabilità

Questa vulnerabilità era particolarmente grave per i seguenti motivi:

- **Remote Exploitation:** Poteva essere sfruttata da remoto senza accesso fisico al sistema.
- **Accesso completo:** Permetteva di bypassare completamente l'autenticazione, esponendo il sistema agli attacchi.
- **Diffusione rapida:** Un attaccante esperto poteva automatizzare l'exploit per colpire un gran numero di server in poco tempo.

Condizioni necessarie

- OpenSSH configurato con autenticazione standard.
- Nessun requisito di configurazioni particolari o di plug-in aggiuntivi.
- Il bug era più facilmente sfruttabile su sistemi con risorse limitate, dove la gestione dei segnali risultava meno prevedibile.

Mitigazioni e difese

Per proteggersi da questa vulnerabilità, Canonical (la casa madre di Ubuntu) ha rilasciato rapidamente un aggiornamento che:

- Corregge l'errata gestione del segnale SIGPIPE.
- Rafforza la logica del processo di autenticazione per prevenire casi di bypass in futuro.

Azioni consigliate:

1. **Aggiornamento immediato**
2. **Log Monitoring**
3. **Firewall**