Newsletter Ubuntu-it

Numero 025 - Anno 2024

Gruppo Social Media

https://wiki.ubuntu-it.org/GruppoPromozione/

2024

Licenza

A cura di:
Daniele De Michele

Newsletter Ubuntu-it

Indice

Questo è il numero **25** del **2024** della Newsletter di Ubuntu-it, riferito alla settimana che va da **lunedì 24 Giugno** a **domenica 30s Giugno**. Per qualsiasi commento, critica o lode, contattaci attraverso la *mailing list* del *gruppo promozione*.

1 Notizie da Ubuntu

1.1 Hai riscontrato problemi con alcune applicazioni su Ubuntu 24.04 LTS? L'aggiornamento di AppArmor potrebbe risolverli

Se anche tu hai riscontrato problemi nell'esecuzione o nel corretto funzionamento di alcune applicazioni in Ubuntu 24.04 LTS, il problema a quanto pare potrebbe essere dovuto a un utilizzo scorretto di *AppArmor* da parte della distribuzione, per limitare la creazione di *namespace* utente. Questo cambiamento, introdotto con questa nuova release, servirebbe per rafforzare la sicurezza del sistema, dato che nessuno vuole che le app nel dispositivo si muovano senza alcun controllo. Però, dall'altra parte i criteri di AppArmor impediscono del tutto l'esecuzione o interrompono le funzionalità di altre app, se non sono configurate ad hoc per AppArmor. Infatti, quando **Canonical** ha introdotto questa modifica, ha osservato che "la fornitura di profili nel pacchetto AppArmor non è (e potrebbe non essere mai) completa" e per questo motivo ha incoraggiato gli sviluppatori a "fornire un profilo AppArmor da distribuire con il loro software per ogni versione di Ubuntu". Ciò richiede tempo e non tutti gli sviluppatori sono disposti a farlo, per questo motivo Ubuntu con il prossimo aggiornamento include e si rende disponibile ad aggiungere eventuali profili dedicati per le app, le varie utility e i servizi annessi. Quindi tieni d'occhio gli aggiornamenti da fare e, se ne hai bisogno, eseguilo il prima possibile, mentre se continui ad avere malfunzionamenti non esitare a farcelo sapere!

Fonte:
omgubuntu.co.uk

2 Notizie dalla comunità internazionale

2.1 Rilasciata la versione di Debian 12.6: scopriamo le novità

Il progetto Debian, dopo quattro mesi di duro lavoro, ha annunciato il rilascio e la disponibilità generale di **Debian 12.6**, come quinta point release per la serie

Bookworm. No, non abbiamo sbagliato scrivendo, poiché la versione di Debian 12.3 non è mai stata rilasciata. Inoltre, c'è una ragione per questo insolito ritardo nel rilascio. Dopo il "dramma", con la scoperta della backdoor su XZ Tarball alla fine di marzo, che ha colpito il ramo Debian, gli sviluppatori hanno deciso di mettere in pausa la versione 12.6 per un'analisi approfondita. Ciò non sorprende, sapendo che Debian è sinonimo di sicurezza senza compromessi, dove nulla viene lasciato incustodito nei minimi dettagli, garantendo la leggendaria stabilità e affidabilità della distribuzione. Tornando a noi, tra gli aggiornamenti degni di nota troviamo:

- Correzioni di sicurezza: vulnerabilità risolte, come problemi di esecuzione di codice remoto in pacchetti come Bluez, Curl e OpenSSL. Queste correzioni garantiscono un utilizzo più sicuro e prevengono potenziali exploit.
- Correzioni di bug: gli sviluppatori hanno corretto svariati problemi, hanno adattato la compatibilità per varie librerie e hanno migliorato la gestione di file system specifici per prevenire la perdita di dati;
- Aggiornamenti dei pacchetti: pacchetti critici aggiornati alle loro ultime versioni, come il kernel Linux, OpenSSL e PostgreSQL, garantendo compatibilità e miglioramenti delle prestazioni.

In numeri, l'aggiornamento Debian 12.6 include un totale di 162 correzioni di bug per pacchetti vari e 84 aggiornamenti di sicurezza. I dettagli su questi aggiornamenti di sicurezza e varie correzioni di bug sono disponibili nella pagina dell'*annuncio del rilascio*. Ultimo, ma che sarebbe primo, questa versione fornisce, su nuovo hardware, un supporto di installazione aggiornato, dal quale non sarà necessario scaricare centinaia di pacchetti dai repository dopo l'installazione. Per finire, gli utenti Debian che non hanno aggiornato le proprie distribuzioni dovrebbero farlo il prima possibile, eseguendo i comandi da terminale:

```
sudo apt update && sudo apt full-upgrade
```

oppure prendere in considerazione un gestore di pacchetti, come Synaptic Package Manager, per poter portare a termine l'aggiornamento.

Fonte:
9to5linux.com
linuxiac.com

3 Notizie dal Mondo

3.1 La nuova veste di Openshot

OpenShot 3.2 è il primo aggiornamento rilasciato al grande pubblico dall'inizio dell'anno scorso e lo stesso sviluppatore capo, *Jonathan Thomas*, descrive questa versione come "rivoluzionaria". Ma andiamo a capire il perché e se effettivamente questa release possa rappresentare un punto di svolta. Partiamo da quello che un utente vede non appena apre l'applicazione, ovvero la presenza

di nuovi temi, che conferiscono a questa versione un aspetto più raffinato e professionale (e in un'era in cui le app di editing mobile-first, come Capcut, alzano il livello di ciò che gli utenti occasionali si aspettano da un'interfaccia utente, questo può essere definito molto importante). Ma saranno le modifiche alle prestazioni, le correzioni di crash e i miglioramenti delle funzionalità a interessare di più i video editor, sia principianti sia esperti. Si è data una maggiore importanza a tutte quelle aree in cui effettivamente Openshot era carente, in modo da limitare, se non colmare, drasticamente il gap con gli altri software di editing. Maggiori dettagli su questo aggiornamento di **OpenShot** sono disponibili direttamente nel sito ufficiale del progetto. Coloro che utilizzano **Ubuntu** (o una sua derivata) potrebbero preferire installare questa nuova versione direttamente dal PPA ufficiale OpenShot, tramite il comando:

```
sudo add-apt-repository ppa:openshot.developers/ppa
sudo apt update && sudo apt install openshot-qt python3-openshot
```

Una volta completata l'installazione, è possibile aprire OpenShot per poterlo utilizzare.

Fonte:
omgubuntu.co.uk
9to5linux.com

3.2 Prima recensione del Raspberry Pi 5 M.2 Hat+

Nel numero *2024.023* della newsletter, abbiamo discusso della tanto attesa novità della Raspberry Pi Foundation per il lancio del componente M.2 Hat per il Raspberry Pi 5, che consente finalmente di avere un'unità disco interna, per una maggiore capacità di archiviazione e un'esperienza di elaborazione dati più veloce. Infatti, l'M.2 Hat promette un trasferimento dati fino a 500 MB/s da e verso le unità NVMe a esso collegate. Non male, vero? Detto questo, nella scatola si trova l'HAT, insieme a una custodia da 16 mm e distanziali filettati per installarlo su una scheda Raspberry Pi 5 che utilizza il Raspberry Pi Active Cooler. Tramite i primi test, si è notato che in termini di velocità, non vi è una differenza sostanziale quando si avvia dall'unità NVMe rispetto all'avvio da un'unità SSD collegata a una porta USB 3.0. Tuttavia, si è notato un piccolo miglioramento rispetto all'avvio da scheda SD. Mentre, come si poteva immaginare, il trasferimento dati è impressionante. Ma non è solo una questione di avvio più veloce o di trasferimento dati più veloce, si tratta anche di avere un'unità disco interna stabile, come hanno tutti i computer. E sì, anche se il Raspberry Pi è progettato per gli amanti della microelettronica che vogliono costruire i propri PC o NAS o qualunque cosa che il Raspberry permetta di fare o di diventare, avere il supporto per l'installazione di un'unità interna è un must.

Fonte:
9to5linux.com

3.3 OpenSSH risolve una vulnerabilità critica

In queste ore gli sviluppatori del progetto **OpenSSH** hanno rilasciato un importante aggiornamento, che permette di risolvere due problemi critici. Il primo,

contrassegnato come (*CVE-2024-6387*), è stato riscontrato nelle versioni di Portable OpenSSH da 8.5p1 a 9.7p1. La vulnerabilità, che potenzialmente consente l'esecuzione di codice arbitrario con privilegi di root, ha colpito in particolare i sistemi Linux a 32 bit con *ASLR*. Sebbene l'exploit non sia stato ancora dimostrato su sistemi a 64 bit, la possibilità purtroppo rimane (per il momento). La seconda correzione, invece, riguarda un errore logico dalle versioni 9.5 alla 9.7, che rendeva inefficace la funzionalità *ObscureKeystrokeTiming*. Questa vulnerabilità potrebbe consentire a un osservatore passivo di rilevare le sequenze di tasti, ponendo un rischio, in particolare quando vengono inserite informazioni sensibili, come le password. A tal proposito, il progetto OpenSSH prevede di eliminare completamente il supporto per l'*algoritmo di firma DSA* entro l'inizio del 2025. Inoltre, con questa versione, appena rilasciata, è stata disabilitata la chiave DSA per impostazione predefinita, a causa delle varie debolezze intrinseche e della tecnologia obsoleta. Ultimo, ma non per importanza, **OpenSSH 9.8** introduce un nuovo sistema di penalità in sshd, bloccando gli indirizzi che mostrano comportamenti sospetti, come ripetuti tentativi di autenticazione falliti. Questa funzionalità mira a migliorare la sicurezza, riducendo il rischio di attacchi brute-force. Oltre a questi miglioramenti, l'aggiornamento include numerose correzioni di bug in tutta la suite di strumenti e alcune modifiche potenzialmente importanti, come la rimozione di alcune funzionalità obsolete e modifiche nel comportamento del server. Per maggiori dettagli dai un'occhiata all'*annuncio di rilascio*.

Fonte:
linuxiac.com
bleepingcomputer.com

3.4 Altra vulnerabilità riscontrata nella maggior parte delle distribuzioni GNU/Linux

Gli sviluppatori Linux stanno risolvendo una vulnerabilità contrassegnata con "alta gravità", che, in alcuni casi, consente l'installazione di malware eseguito a livello di firmware, consentendo di accedere alle parti più profonde di un dispositivo, in cui è difficile individuare/rimuovere un virus. La vulnerabilità in questione, tracciata come *CVE-2023-40547*, risiede in shim (creato anch'esso dalla comunità per beneficiare dei vantaggi del Secure Boot), che nel contesto di Linux è un piccolo componente eseguito nel firmware all'inizio del processo di avvio della macchina, prima che il sistema operativo venga avviato. Più specificamente, lo shim che accompagna praticamente tutte le distribuzioni Linux svolge un ruolo cruciale nell'avvio sicuro della distribuzione, una protezione integrata nella maggior parte dei dispositivi informatici moderni per garantire che ogni collegamento nel processo di avvio provenga da un fornitore verificato e affidabile. Lo sfruttamento riuscito della vulnerabilità consente agli aggressori di neutralizzare questo meccanismo, eseguendo firmware dannoso nelle prime fasi del processo di avvio. La correzione della vulnerabilità comporta più che la semplice rimozione del buffer overflow dal codice shim, anche l'aggiornamento del meccanismo di avvio sicuro per revocare le versioni vulnerabili del bootloader. Ciò, a sua volta, aumenta un certo livello di rischio. *Paul Asadoorian*, principale specialista della sicurezza presso *Eclypsium* spiega inoltre come un'altra sfida nell'aggiornamento riguarda la quantità limitata di spazio riservato per l'archi-

viazione delle revoche in una porzione dell'UEFI nota come DBX. Alcuni elenchi potrebbero contenere più di duecento voci, che devono essere aggiunte al DBX, che a sua volta potrebbe portare all'esaurimento dello spazio. Ancora un altro passaggio nel processo di patch è la firma degli shim appena corretti utilizzando un'autorità di certificazione di terze parti Microsoft. Detto questo, il danno derivante dallo sfruttare una vulnerabilità di questo tipo è contrassegnata con un punteggio di 9,8 su 10. Per questo motivo, tutti gli utenti dovrebbero installare tempestivamente le patch non appena diventano disponibili per le proprie distribuzioni.

Fonte:
arstechnica.com

4 Aggiornamenti e statistiche

4.1 Aggiornamenti di sicurezza

Gli annunci di sicurezza sono consultabili nell'apposita *sezione del forum*.

4.2 Bug riportati

- Aperti: 144141, **-46** rispetto alla scorsa settimana.
- Critici: 307, **-1** rispetto alla scorsa settimana.
- Nuovi: 72667, **-35** rispetto alla scorsa settimana.

È possibile aiutare a migliorare Ubuntu, riportando problemi o malfunzionamenti. Se si desidera collaborare ulteriormente, la *Bug Squad* ha sempre bisogno di una mano.

5 Commenti e informazioni

La tua newsletter preferita è scritta grazie al contributo libero e volontario della *comunità ubuntu-it*. In questo numero hanno partecipato alla redazione degli articoli:

- *Daniele De Michele*

Ha inoltre collaborato all'edizione:

- *Stefano Dall'Agata*

Ha realizzato il pdf:

- *Daniele De Michele*

6 Scrivi per la newsletter

La **Newsletter Ubuntu-it** ha lo scopo di tenere aggiornati tutti gli utenti **Ubuntu** e, più in generale, le persone appassionate del mondo open-source. Viene resa disponibile gratuitamente con cadenza settimanale ogni Lunedì, ed è aperta al contributo di tutti gli utenti che vogliono partecipare con un proprio articolo. L'autore dell'articolo troverà tutte le raccomandazioni e istruzioni dettagliate all'interno della pagina *Linee Guida*, dove inoltre sono messi a disposizione per tutti gli utenti una serie di indirizzi web che offrono notizie riguardanti le principali novità su Ubuntu e sulla comunità internazionale, tutte le informazioni sulle attività della comunità italiana, le notizie sul software libero dall'Italia e dal mondo. Per chiunque fosse interessato a collaborare con la newsletter Ubuntu-it a titolo di redattore o grafico, può scrivere alla *mailing list* del *gruppo promozione* oppure sul canale IRC: *#ubuntu-it-promo*. Fornire il tuo contributo a questa iniziativa come membro, e non solo come semplice utente, è un presupposto fondamentale per aiutare la diffusione di Ubuntu anche nel nostro paese. Per rimanere in contatto con noi, puoi seguirci su:


Facebook


Twitter


YouTube


Telegram

"Noi siamo ciò che siamo per
merito di ciò che siamo tutti"

Questa newsletter è stata prodotta dal
Gruppo Social Media usando esclusivamente
software libero.