Newsletter Ubuntu-it

Numero 017 - Anno 2023

Gruppo Social Media

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

2023

Licenza

Questo documento è stato composto interamente dall'autore con LaTeX. Per maggiori informazioni, o segnalazioni:

Mailing List Newsletter-italiana: iscriviti per ricevere la Newsletter Italiana di Ubuntu!;
Mailing List Newsletter-Ubuntu: la redazione della newsletter italiana. Se vuoi collaborare alla realizzazione della newsletter, questo è lo strumento giusto con cui contattarci.
Canale IRC: *#ubuntu-it-promo*

A cura di:
Daniele De Michele

Newsletter Ubuntu-it

Indice

Questo è il numero **17** del **2023** della Newsletter di Ubuntu-it, riferito alla settimana che va da **lunedì 1 Maggio** a **domenica 7 Maggio**. Per qualsiasi commento, critica o lode, contattaci attraverso la *mailing list* del *gruppo promozione*.

1 Notizie da Ubuntu

1.1 Sono disponibili le prime build giornaliere di Ubuntu 23.10

Dopo aver dato il via libera allo sviluppo di **Ubuntu 23.10 (Mantic Minotaur)**, ora **Canonical** ha pubblicato le prime immagini *.iso* per tutti gli utenti e sviluppatori che desiderano cavalcare l'onda e stare al passo con lo sviluppo della distribuzione e vogliono anche testarla. Come previsto, queste prime build giornaliere di Ubuntu 23.10 sono basate ancora sulla precedente versione di Ubuntu (la 23.04), arrivata per le strade il mese scorso e più precisamente il 20 aprile. Questo significa che vengono forniti praticamente gli stessi componenti principali della versione precedente, sia che riguardi il kernel Linux, sia l'ambiente desktop che le relative applicazioni preinstallate.
Durante questo ciclo di sviluppo di sei mesi, le build giornaliere verranno aggiornate con alcune delle più recenti tecnologie GNU/Linux e relativi software open source, come l'imminente ambiente desktop GNOME 45, lo stack grafico Mesa 23.1 o ancora il kernel Linux 6.5. Senza ulteriori indugi, è possibile scaricare le prime immagini *.iso* di **Ubuntu 23.10** direttamente dal *server* ufficiale di Ubuntu (stessa cosa vale per le principali derivate, come Kubuntu, Xubuntu, Lubuntu, etc). Stando attenti che, essendo delle build giornaliere, ovvero immagini istantanee prodotte quotidianamente, queste sono destinate a una fascia ristretta di utenti che desiderano eseguire test o sviluppo. Quindi, qualora si voglia procedere con l'installazione, è raccomandato lo si faccia o in una macchina virtuale o in un dispositivo da non utilizzare nella quotidianità.

Fonte:
omgubuntu.co.uk
9to5linux.com

1.2 Vuoi più sfondi per il tuo desktop? Installa gli sfondi GNOME

Tutte le distribuzioni **Ubuntu** vengono fornite con una piccola raccolta/selezione di sfondi pronti all'uso. La scelta purtroppo non è né vasta né varia e a un certo

punto vi stancherete di vedere sempre le solite immagini e vi immergerete nella ricerca di nuovi sfondi per far riprendere vita al vostro desktop. Bene, un modo semplice e veloce per aggiungere rapidamente altri sfondi di alta qualità alla vostra distribuzione Ubuntu è installare il pacchetto *gnome-backgrounds*, presente nei repository ufficiali. La maggior parte degli *sfondi* forniti dagli sviluppatori **GNOME** è disponibile in coppie chiaro/scuro (vi è buona varietà di contenuti: da sovrapposizioni geometriche a illustrazioni 3D straordinariamente dettagliate). Questo cambiamento dipenderà dalle impostazioni di base selezionate nelle vostre preferenze e funzionerà in modo tale che, se la modalità chiara è attiva, otterrete la versione mostrata sul lato sinistro dell'anteprima della miniatura, mentre quando la modalità scura è attiva, si passerà all'anteprima sul lato destro. Quindi, anziché perdere tempo nel navigare sul web senza alcun risultato, affidati al buon gusto del progetto GNOME!

Fonte:
omgubuntu.co.uk

1.3 Trick del mese: aggiungere il pannello audio nelle Impostazioni rapide di Ubuntu 23.04

L'ultima versione dell'ambiente desktop **GNOME 44** ha sorpreso il grande pubblico per tutte quelle ottimizzazioni integrate nelle "Impostazioni rapide". Alcune di queste andranno ancora perfezionate senza alcuna ombra di dubbio, come per esempio il gestore dei controlli multimediali, che risulta un applet separato. Allora, viene in soccorso in questo caso, una nuova estensione chiamata *Quick Settings Audio Panel*, il cui compito è abbastanza semplice: crea una sezione dedicata all'audio nel menu delle impostazioni rapide e sposta in questa sezione i controlli relativi all'audio. L'estensione è in grado di mostrare i flussi audio associati a ogni applicazione, in modo da poter gestire il volume indipendentemente dal flusso audio principale. È possibile anche scegliere dove posizionare il pannello audio, stando attenti a un relativo "problema", in quanto è necessario disabilitare/abilitare l'estensione dopo aver apportato le dovute modifiche nel pannello delle impostazioni dell'estensione affinché tali modifiche abbiano effetto. Per finire, *Quick Settings Audio Panel* è presente nella pagina *GNOME extensions* ed è possibile installarla su **Ubuntu 23.04** oppure su qualsiasi altra distribuzione Linux che includa GNOME 44.

Fonte:
omgubuntu.co.uk

1.4 Basi di sicurezza dei Big Data: Storia e Framework

Tutti quanti abbiamo letto i vari titoli di giornali su spettacolari violazioni dei dati e altri incidenti di sicurezza e l'impatto che hanno avuto sulle organizzazioni vittime. Da LastPass a SolarWinds, la "sicurezza dei dati" sembra essere la frase che più spesso esce dalla bocca di ogni *CTO* in questo ultimo periodo. E per certi versi non esiste luogo più vulnerabile agli attacchi di un ambiente di *big data*, come un *data lake*, che altro non è che un repository centralizzato progettato per archiviare, elaborare e proteggere grandi quantità di dati strutturati. Infatti, i

sistemi ad alta quantità di dati sono stati oggetto di innumerevoli attacchi, tra i più memorabili citiamo:

- Nell'incidente di **Log4Shell**, è stato scoperto che si poteva aprire una backdoor remota, che concedeva all'aggressore l'accesso alla riga di comando sul sistema, tramite alcune versioni della popolare e ampiamente utilizzata libreria di registrazione log4j. Alla vulnerabilità è stato assegnato un *punteggio CVSS* di 10/10 da parte di *Apache Software Foundation* (il manutentore di Log4j);

- **Heartbleed** era un exploit scovato nelle versioni precedenti della libreria OpenSSL, che è un'implementazione ampiamente usata del protocollo TLS. Consentiva agli aggressori, tra le altre cose, di intercettare le comunicazioni. La vulnerabilità è stata ampiamente sfruttata ed è stata un fattore chiave nella compromissione di numerosi ambienti di dati critici, tra cui le cartelle cliniche di *oltre quattro milioni* di cittadini statunitensi;

- Con **ShellShock**, gli aggressori sono stati banalmente in grado di sfruttare una vulnerabilità nella shell bash di Linux per ottenere il totale controllo sul sistema bersaglio. In alcuni scenari, ciò potrebbe essere ottenuto da remoto, ad esempio se il sistema dispone di un server con il supporto degli script CGI abilitato. Anche in questo caso, la vulnerabilità è stata ampiamente sfruttata dagli aggressori di tutto il mondo.

Tuttavia, gli aggressori possono avere molte intenzioni e i loro attacchi possono presentarsi in molte forme, come un:

- **Worm di criptojacking**, che si verifica quando un utente malintenzionato sfrutta il sistema di destinazione per eseguire attività di mining di criptovalute non autorizzate, per valute come Monero. Sistemi di big data, come Hadoop, Kubernetes, MongoDB ed !ElasticSearch, sono stati tutti l'obiettivo di worm di cryptojacking, come *PsMiner* (malware virale che sfrutta le vulnerabilità del sistema per diffondersi senza l'interazione dell'utente), per eseguire il mining di criptovaluta su larga scala, utilizzando le risorse parallele e distribuite del cluster. Sebbene il malware di cryptojacking potrebbe non esporre immediatamente i dati al rischio di una violazione, il malware può abusare delle risorse di un cluster su larga scala;

- **Cripto-ransomware**. In questo tipo di attacco, i file system e i database del computer della vittima vengono crittografati dal malware. L'attaccante estorce quindi un riscatto per decrittare i dati della vittima. Esempi passati includevano CryptoLocker e WannaCry;

- **APT e spionaggio (aziendale)**, in cui, a parte il furto di dati, l'estorsione degli utenti e l'abuso di risorse, le minacce persistenti avanzate (APT in breve) sono messe in atto da aggressori che si infiltrano nelle reti di un'organizzazione a lungo termine. Potrebbero esserci molte ragioni per farlo, ma una ragione comune è lo spionaggio, che si tratti di spionaggio aziendale in un contesto commerciale o di un vero e proprio spionaggio nei settori pubblici, ONG, non-profit o del settore legale.

Quando i dati provenienti da tutta l'organizzazione vengono aggregati in un data lake o in un sistema di big data simile, possono costituire un obiettivo molto attraente per le attività di raccolta di informazioni APT e un'interessante fonte di dati per l'esfiltrazione. In questo caso si parla di violazione dei dati e si verifica quando i dati vengono esfiltrati e divulgati in modo non autorizzato. Una violazione dei dati può variare in scala, ad esempio, pubblicando erroneamente informazioni di identificazione personale su una intranet aziendale. O esponendo maliziosamente i registri finanziari di decine di milioni di clienti bancari.

È facile capire che c'è molto in gioco, e anche se il proprio data lake o altra soluzione per big data non gestisce dati sensibili, c'è comunque il rischio che possa cadere vittima di uno degli attacchi sopra citati, se non si prendono misure di sicurezza sufficienti per proteggere adeguatamente l'ambiente di trattamento dei dati. Un buon punto di partenza è la modellazione delle minacce e uno dei framework più popolari per questo è **STRIDE**. Un framework di valutazione delle minacce originariamente concepito alla fine degli anni '90, che può essere utilizzato per prendere decisioni riguardanti i controlli di sicurezza che occorre implementare per proteggere i propri dati. STRIDE è un acronimo e le lettere della parola stanno per (tradotte dall'inglese):

- S = *Spoofing*, che significa ingannare il sistema bersaglio fingendo di essere un altro utente.
- T = Manomissione, che significa alterare il sistema di destinazione, come i registri di sistema o i dati gestiti dal sistema.
- R = Rinnegare, che significa rimuovere qualsiasi traccia o prova che il sistema di destinazione sia stato illegittimamente accessibile o manomesso.
- I = *Divulgazione di informazioni*, che significa far sì che il sistema target divulghi informazioni, come i dati che gestisce, in maniera non autorizzata.
- D = *Negazione del servizio*, che significa rendere il sistema di destinazione non disponibile, ad esempio bloccando il sistema o sovraccaricandolo con miliardi di richieste.
- E = *Elevazione dei privilegi*, che significa ottenere ulteriori privilegi di accesso non autorizzato sul sistema di destinazione, ad esempio, raggiungere i permessi di root.

Il processo che i team devono seguire per una valutazione STRIDE, in genere, inizia con la creazione di una serie di diagrammi di sistema, che spiegano come esso funzioni e come si integri con altri sistemi nel suo contesto operativo. Nel prossimo numero della newsletter, analizzeremo i cinque controlli di sicurezza best practice fondamentali che possono aiutare a proteggere qualsiasi ambiente di elaborazione dati su larga scala.

Fonte:
ubuntu.com

2 Notizie dal Mondo

2.1 HuggingChat: prima alternativa open source a ChatGPT

Dopo che ChatGPT è stata "bannata" in Italia (notizia di questi giorni, per chi non lo sapesse, è stata riaperta la piattaforma dopo che OpenAI, l'azienda proprietaria, si è allineata alle richieste del garante della privacy italiano, che chiedeva più trasparenza e privacy per gli utenti del servizio), i vari utenti si sono rimboccati le maniche per trovare una rapida soluzione. Tra queste vi era l'utilizzo di una VPN (Virtual Private Network) per aggirare le restrizioni imposte, ma questo non è il caso di cui vogliamo parlare oggi. Perché di recente è stato rilasciato un nuovo modello linguistico di grandi dimensioni (LLM) basato su *Open Assistant*, chiamato *HuggingChat*, che si prefigge l'obiettivo principale di fornire un'alternativa più trasparente, inclusiva e responsabile rispetto a ChatGPT. Fondamentalmente, nel suo stato attuale, HuggingChat funge da interfaccia utente, facilitando l'interazione con il chatbot. Inoltre, essendo ancora in una prima fase di sviluppo, è carente di alcune funzionalità chiave, come il salvataggio della conversazione al riavvio del browser o quando lo si cambia. Soffre anche di alcuni errori familiari durante l'esecuzione, come: "Troppo traffico, riprova più tardi". Non è ancora ai livelli di ChatGPT, ma alternative open source, come queste, hanno bisogno del giusto tempo per progredire e forse un giorno non troppo lontano competere coi suoi concorrenti.

Fonte:
news.itsfoss.com

2.2 Pronto nuovo codice Rust per il Kernel Linux 6.4

Abbiamo discusso nei precedenti numeri della newsletter di come il linguaggio di programmazione *Rust*, a piccolo passi, stia entrando sempre di più nel far parte del kernel Linux. A tal proposito, venerdì scorso, uno degli sviluppatori principali di Rust, Miguel Ojeda, ha presentato una richiesta di *pull* per alcune nuove funzionalità che faranno parte della prossima versione del kernel Linux, più precisamente l'introduzione delle API pin-init, di cui un esempio del codice sottostante:

```
#[pin_data]
struct Example (
#[pin]
valuet Mutex<u32>,

#[pin]
value_changed: CondVar,
}

impl Example (
fn new()-> impl PinInit<self {
pin_init!(Self (
value <- new_mutex.(0),
value_changed <- new_condvar!(),
```

```
})
}
}

// In ‘Box‘.
let b= Box: pin_init(Example::new())?;

// In the stack.
stack. pin_inith!(let s = Example::new());
```

In particolare, questa implementazione serve per gestire nel migliore dei modi l'inizializzazione sicura dei pin e consente di ridurre la quantità di codice Rust "non sicuro" all'interno del kernel in merito alle strutture di dati che richiedono un indirizzo stabile. La nuova API pin-init a sua volta sarà utilizzata anche da altre imminenti funzionalità di Rust per Linux.

Fonte:
phoronix.com

2.3 I nuovi comandi sudo e su, scritti in Rust

Le imminenti funzionalità di cui parlavamo nell'articolo precedente sono racchiuse in una recente pubblicazione rilasciata dal sito *Memory Safety*, su cui viene annunciata la nuova implementazione dei comandi *sudo* e *su* attraverso il linguaggio di programmazione *Rust*. Prima però ci soffermiamo su un po' di storia, perché è utile ricordare che il comando *Sudo* è stato sviluppato per la prima volta negli anni '80 e, nel corso dei decenni, è diventato uno strumento essenziale per eseguire modifiche riducendo al minimo i rischi all'interno di un sistema operativo. Ma poiché è scritto in *C*, *sudo* ha riscontrato in questi anni molte vulnerabilità legate a problemi di sicurezza della memoria. Per questo, quando pensiamo ai rischi che un software può comportare quando è in esecuzione nel nostro dispositivo, pensiamo a:

1. La sua diffusione;
2. La sua importanza;
3. Quali funzioni critiche svolge;
4. Se il linguaggio utilizzato è insicuro per la memoria (es. C, C++, asm).

È facile capire come *sudo* soddisfi tutti i quattro criteri di rischio appena citati. Allora, è importante proteggere tutti i software che sono maggiormente esposti a questi rischi, in particolare dalle vulnerabilità di sicurezza della memoria. Ed è qui che entra in gioco Rust, con le sue peculiarità, che permettono di arginare e risolvere parte di questi problemi. Detto questo, se anche tu sei curioso di vedere come procedono i lavori oppure desideri contribuire, su *GitHub* è presente la *pagina del progetto*. Nessuno vieta la possibilità di implementarli nel proprio ambiente di lavoro (sempre con le dovute raccomandazioni del caso).

Fonte:
memorysafety.org

2.4 LibreOffice 7.5.3 è pronto per il downaload

La **Document Foundation** ha *annunciato* il rilascio e la disponibilità per tutte le piattaforme supportate della sesta point release della versione stabile della potente suite per l'ufficio, **LibreOffice 7.5**. Questa versione scende in campo per risolvere con esattezza 119 bug, presenti all'interno di tutti i componenti principali della suite per l'ufficio, inclusi Writer, Calc, Impress e Draw. Queste correzioni permettono di aumentare sempre di più la stabilità e la robustezza della suite, garantendo al contempo una migliore interoperabilità con i formati di documenti proprietari della suite MicroSoft Office, come DOCX, XLSX e PPTX. Pertanto, se all'interno del tuo dispositivo utilizzi la versione di LibreOffice 7.5, dovresti prendere in considerazione l'aggiornamento alla versione 7.5.3 il prima possibile e magari dare anche un'occhiata ai dettagli sulle correzioni di questi bug, disponibili per *RC1* e *RC2*. Tuttavia, occorre tenere presente che questa è l'edizione "Community", quindi se hai bisogno di supporto per le distribuzioni aziendali dovresti considerare l'utilizzo della famiglia di applicazioni *LibreOffice Enterprise* (per maggiori informazioni guarda il numero *2021.005*).
LibreOffice 7.5.3 è immediatamente disponibile sul *sito ufficiale*. I requisiti minimi per i sistemi operativi proprietari sono disponibili nella *suddetta pagina*; mentre per **GNU/Linux**, si ricorda principalmente come regola generale che è sempre consigliabile installare LibreOffice utilizzando i metodi di installazione raccomandati dalla propria distribuzione, come ad esempio l'uso di **Ubuntu Software Center** per **Ubuntu**. Gli utenti di LibreOffice, i sostenitori del software libero e i membri della comunità possono supportare The Document Foundation attraverso una *piccola donazione*. Le vostre donazioni aiutano **The Document Foundation** a mantenere la sua infrastruttura, condividere la conoscenza e a finanziare attività delle comunità locali.

Fonte:
9to5linux.com

2.5 Nuova app di intelligenza artificiale per i sistemi Linux

I temi riguardanti l'intelligenza artificiale stanno diventando sempre più frequenti, ormai non si sente più parlare d'altro. Dai telefoni alle macchine sino ad arrivare ai computer con sistemi integrati per dare spazio alle funzionalità riguardanti l'AI. Ma in tutto questo vi è un'applicazione desktop anche per i sistemi GNU/Linux, senza dover necessariamente aprire un browser? Questo è ciò che si sono chiesti alcuni utenti della comunità, che navigando su Internet hanno avuto un incontro ravvicinato con *Bavarder*, un'applicazione scritta in Python e ottimizzata con GTK4/libadwaita. L'interfaccia utente è incredibilmente semplice e permette, in un'apposita casella, di scrivere la propria query e, una volta aver premuto il pulsante blu di invio, attendere qualche istante per ricevere la risposta cercata. Al momento del test, **Bavarder** utilizza *BAI Chat*, un chatbot basato su API GPT-3.5/ChatGPT, che può essere utilizzato gratuitamente, senza bisogno di registrazioni o chiavi API. Un recente aggiornamento dell'app aggiunge il supporto per backend alternativi, come ChatGPT 4 e Hugging Chat, sebbene alcuni di questi richiedano l'inserimento di una chiave API. Non c'è invece al momento alcuna opzione per rigenerare una risposta, poiché non esiste una visualizzazione delle cronologie delle "conversazioni" (cosa che

invece fa ChatGPT), e quindi risulta difficile tenere traccia di una conversazione o iterare e dare seguito alle risposte.
Qui si applicano i soliti avvertimenti su questo tipo di tecnologie, infatti le risposte possono sembrare convincenti, ma potrebbero contenere informazioni inesatte o false. È anche abbastanza facile ingannare questi modelli in loop illogici, come convincerli che 2 + 2 = 106, quindi occorre fare attenzione e ricordarsi di avere un cervello che funziona! Oltre a questo, **Bavarder** è un'app dall'aspetto eccezionale ,con uno tema chiaro e pulito e soprattutto ben definito. Se sei un fan di ChatGPT e simili, vale la pena dare un'occhiata e visitare la pagina su *Flathub*.

Fonte:
omgubuntu.co.uk

3 Aggiornamenti e statistiche

3.1 Aggiornamenti di sicurezza

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

3.2 Bug riportati

- Aperti: 141977, +**35** rispetto alla scorsa settimana.
- Critici: 312, = rispetto alla scorsa settimana.
- Nuovi: 71297, +**4** 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.

4 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*
- *Massimiliano Arione*

Ha realizzato il pdf:

- *Daniele De Michele*

5 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.