Newsletter Ubuntu-it

Numero 019 - Anno 2022

Gruppo Social Media

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

2022

Licenza

A cura di:
Daniele De Michele

Newsletter Ubuntu-it

Indice

Questo è il numero **19** del **2022** della Newsletter di Ubuntu-it, riferito alla settimana che va da **lunedì 16 Maggio** a **domenica 22 Maggio**. Per qualsiasi commento, critica o lode, contattaci attraverso la *mailing list* del *gruppo promozione*.

1 Notizie dalla comunità internazionale

1.1 Rilasciato un nuovo aggiornamento di sicurezza da parte di Canonical

In queste ore, **Canonical** ha rilasciato una serie di patch di sicurezza per il Kernel Linux, per metter fine a una serie di vulnerabilità, più precisamente 17, riscontrate sulle versioni di Ubuntu 21.10 (Impish Indri), Ubuntu 20.04 LTS (Focal Fossa), Ubuntu 18.04 LTS (Bionic Beaver), nonché Ubuntu 16.04 e 14.04 ESM. L'unica eccezione riguarda Ubuntu 22.04 LTS (Jammy Jellyfish), che ha già ricevuto il suo primo aggiornamento del kernel la scorsa settimana (per maggiori informazioni *2022.016*). Ma tornando a noi, il nuovo aggiornamento di sicurezza per tutte le versioni di Ubuntu risolve un difetto (*CVE-2021-26401*), scoperto dai ricercatori Ke Sun, Alyssa Milburn, Henrique Kawakami, Emma Benoit, Igor Chervatyuk, Lisa Aichele e Thais Moreira Hamasaki nelle mitigazioni della seconda variante di *Spectre* per i processori AMD, che potrebbero consentire a un utente malintenzionato locale di esporre informazioni riservate. Si corregge anche un problema (*CVE-2022-25258*) scoperto nel sottosistema del gadget USB, che potrebbe consentire a un utente malintenzionato di causare un arresto anomalo del sistema, un difetto (*CVE-2022-25375*) scoperto nel *driver NFC ST21NFCA*, che potrebbe consentire a un utente malintenzionato fisicamente vicino al dispositivo di eseguire del codice arbitrario, nonché una vulnerabilità (*CVE-2022-25375*) scoperta nell'implementazione del gadget USB Remote NDIS (RNDIS), che potrebbe consentire a un utente malintenzionato di esporre dati sensibili.

Mentre, per i soli sistemi Ubuntu 21.10, 20.04 LTS e 18.04 LTS, viene risolta una vulnerabilità (*CVE-2022-27223*) scoperta nel driver del dispositivo USB2 Xilinx, che potrebbe consentire a un utente malintenzionato fisicamente vicino di mandare in crash il sistema. Invece, per i sistemi Ubuntu 21.10, 20.04 LTS e 18.04 LTS che eseguono il kernel Linux 5.4 LTS, si risolve un difetto (*CVE-2022-20008*) scoperto nel sottosistema MMC/SD del kernel Linux, che potrebbe consentire a un utente malintenzionato di esporre informazioni sensibili e altri due bug, il primo (*CVE-2022-1016*) scoperto da David Bouman nel sottosi-

stema netfilter, consente a un utente malintenzionato locale di esporre informazioni riservate, mentre il secondo riguarda una vulnerabilità (*CVE-2020-27820*) use-after-free, scoperto da Jeremy Cline nel driver grafico nouveau, che potrebbe consentire a un utente malintenzionato privilegiato un arresto anomalo del sistema.

Inoltre, solo per i sistemi Ubuntu 18.04 LTS che eseguono il kernel Linux 4.15, abbiamo una vulnerabilità (*CVE-2022-24958*) use-after-free scoperta nell'interfaccia del file system USB Gadget, che potrebbe consentire a un utente malintenzionato locale di causare un arresto anomalo del sistema o ancora eseguire del codice arbitrario, nonché una serie di difetti (*CVE-2022 -23036*, *CVE-2022-23037*, *CVE-2022-23038*, *CVE-2022-23039*, *CVE-2022-23040* e *CVE-2022-23042*) scoperti da Demi Marie Obenour e Simon Gaiser nei frontend dei dispositivi di paravirtualizzazione Xen, che potrebbero consentire a un utente malintenzionato di accedere alle pagine di memoria di una macchina virtuale guest. Per concludere, consigliamo vivamente a tutti gli utenti di aggiornare quanto prima i propri dispositivi, ricordando che, per farlo, basterà aprire una finestra di terminale e digitare il seguente comando:

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

oppure utilizzare la classica app *Ubuntu Software*. Poiché si tratta di un aggiornamento del kernel, ricorda di riavviare il sistema dopo aver installato con successo la nuova versione del kernel.

Fonte:
9to5linux.com

1.2 App Flatpak della settimana: Pika Backup: proteggere i tuoi dati non è mai stato così facile

L'applicazione scelta questa settimana da parte della comunità è **Pika Backup**, una simpatica utility creata da Sophie Herold che, con una semplice e intuitiva interfaccia grafica, permette di eseguire i backup dei propri dati in modo sicuro, senza copiare più e più volte i dati sul disco. Lo strumento è scritto in *GTK4* e ha un'interfaccia moderna, che si adatta ai temi scuri o chiari della propria distribuzione ed è ricco di svariate opzioni. Infatti, è possibile creare backup in locale sulla stessa macchina (sconsigliato), su un driver esterno, come una chiavetta USB o un disco SSD/HDD o ancora su un'unità remota sulla tua rete locale, o su un host remoto accessibile tramite SSH. I backup possono essere programmati a intervalli orari, giornalieri, settimanali o mensili a una determinata ora ed è possibile suggerire all'applicazione di eliminare regolarmente i vecchi archivi di backup, quando questi non servono più. Non può mancare di certo la parte riguardante la crittografia con password dei propri backup e la possibilità di elencare gli archivi di backup creati e sfogliarne i contenuti. Mantenere i dati al sicuro non è mai stato così facile con **Pick Backup** e si può installare nella propria distribuzione GNU/Linux come app Flatpak dal repository *Flathub* o tramite l'App Store.

Fonte:
9to5linux.com

1.3 Canonical recluta personale per il team "Ubuntu Gaming"

Nel numero *2022.016* della newsletter, abbiamo parlato di come **Canonical** si stia impegnando per portare stabilità, affidabilità ed elevate prestazioni nel gaming nella distribuzione Ubuntu. Per farlo, ha deciso in primo luogo di presentare al grande pubblico il pacchetto snap dell'app Steam, per eseguire i primi test pubblici. Ora, però, Canonical è alla *ricerca* di figure di software engineer, che si uniscano al team *Ubuntu Gaming Experience*. Nell'annuncio di lavoro, la stessa Canonical scrive:

> *"Siamo in un momento emozionante per i giochi su Linux. Strumenti di compatibilità come Proton sono maturati e molti titoli di giochi che girano su Windows possono essere fatti funzionare, espandendo enormemente la libreria di titoli disponibili su Linux. Offrire un'esperienza di gioco completa non è solo compatibilità; si tratta di massimizzare le prestazioni su un'ampia gamma di hardware, garantire che l'anti-cheat sia robusto e sicuro, semplificare l'accesso agli strumenti per la creazione di contenuti, la gestione dei driver e le sovrapposizioni HUD, oltre a garantire che controller di gioco, cuffie, tastiere RGB e mouse da gioco siano completamente supportati e personalizzabili".*

Si capisce che c'è tanto lavoro da fare. Per questo motivo, chi deciderà di inviare la candidatura dovrà mettere in conto che dovrà conoscere la tecnologia integrata dei moderni giochi Linux, come ad esempio esperienza di suono, grafica, input e avere anche una certa familiarità o interesse per OpenGL, Vulcano, MESA, Vino, eccetera. Per concludere, ancora una volta, la società di *Mark Shuttleworth* sta investendo nella comunità, con assunzioni, progetti ed eventi (come il ripristino dell'**Ubuntu Developer Summit**, di cui abbiamo parlato nel numero *2022.017*), ma anche nella modernizzazione del desktop per tutte quelle ambizioni più ampie, che arriveranno con la versione 22.10 e oltre.

Fonte:
omgubuntu.co.uk

1.4 Ubuntu Preview su WSL: ecco cosa c'è in serbo

Sulla scia del rilascio di **Ubuntu 22.04 LTS**, si è iniziato lo sviluppo e la creazione delle prime immagini per la nuova versione di **Ubuntu 22.10**. Mentre gli utenti che utilizzano Ubuntu WSL hanno avuto accesso solo alle attuali versioni *Long Term Supported (LTS)*, che forniscono agli sviluppatori che si occupano di data science, cloud, web e IoT un ambiente di sviluppo stabile e profondamente integrato con Windows. Però, sta aumentando sempre più la richiesta degli utenti che vogliono ricevere subito l'innovazione e dopo la stabilità (con tutti i pro e i contro). Allora **Canonical**, per venire incontro a queste richieste da parte della comunità, ha dato il via allo sviluppo di *Ubuntu Preview*, che permette di provare gli ultimi aggiornamenti e miglioramenti introdotti nelle build giornaliere direttamente sul proprio computer Windows. Per quanto sorprendente possa sembrare, anche se in realtà non lo è, questa versione non è adatta ad un uso quotidiano, infatti potrebbero essere presenti dei bug. Ma se vuoi dare una

sbirciatina ai progressi di **Ubuntu** o ancora aiutare la comunità a identificare problemi e miglioramenti, potrebbe essere l'app che fa per te. Siamo ansiosi di ascoltare le vostre esperienze e di vedere i vostri feedback o segnalazioni su *Discourse*.

Fonte:
ubuntu.com

2 Notizie dal Mondo

2.1 Un grande passo in avanti da parte della Software Freedom Conservancy per i diritti open source

Un importante passo in avanti per i diritti della comunità open source si sta svolgendo in questi giorni in America. La *Software Freedom Conservancy (SFC)*, ovvero un'organizzazione senza scopo di lucro che promuove il software open source e, tra le altre cose, difende anche la *General Public License (GPL)*, licenza del software libero, ha recentemente citato in giudizio il principale fornitore di TV *Vizio*, per aver abusato della GPL con il suo sistema *SmartCast OS*, basato su Linux. La SFC ha sporto la sua denuncia, affermando che Vizio, all'interno del firmware del suo sistema SmartCast OS TV, utilizza del codice sorgente dedicato a software open source, come BusyBox, U-Boot, bash, gawk, tar, Glibc e FFmpeg. Siccome questi programmi sono protetti dalla GPLv2 e dalla LGPL, i consumatori, e non solo gli sviluppatori, hanno il diritto di modificare, migliorare, condividere e reinstallare le versioni modificate del software. Lo stesso direttore esecutivo della SFC, a tal proposito, ha dichiarato e spiegato come: *"La sentenza è un momento spartiacque nella storia delle licenze copyleft. Questa sentenza mostra che gli accordi GPL funzionano sia come licenze di copyright sia come accordo contrattuale. Per questo chiediamo al tribunale di richiedere a Vizio di adempiere ai propri obblighi, in base ai requisiti di conformità del copyright"*. In questa causa, la **SFC** non chiede soldi, ma solamente che Vizio fornisca il codice sorgente a tutti i clienti che acquistano i suoi prodotti.

Fonte:
zdnet.com

2.2 Microsoft avverte: scoperta nuova Botnet che prende di mira i sistemi Linux

I ricercatori di **Microsoft** di recente hanno individuato una nuova variante della botnet **Sysrv**, che prende di mira un difetto critico nello *Spring Framework* (*CVE-2022- 22947*) e che permette di installare malware ad hoc riguardante il mining di crypto su sistemi Linux e Windows. In particolare, il difetto ha interessato lo Spring Cloud Gateway di **VMware** e la Communications Cloud Native Core Network Exposure Function di **Oracle**. Inoltre, in un *thread* pubblicato su Twitter, il team Security Intelligence di Microsoft ha dichiarato che la botnet esegue una scansione di Internet prima di individuare i server web, in cui poi successivamente utilizza una serie di vulnerabilità per portare a termine l'attacco. Una volta che il malware è all'interno e in esecuzione, usufruisce

delle risorse della macchina stessa per eseguire mining di cryptovalute. Non solo, perché con questa variante può anche acquisire le credenziali del database, per controllare l'intero server. Le raccomandazioni, in questi casi, riguardano l'applicazione costante degli aggiornamenti di sicurezza dei vari produttori e l'aumento della sicurezza delle proprie credenziali.

Fonte:
zdnet.com

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: 139320, +**49** rispetto alla scorsa settimana.
- Critici: 326, **-10** rispetto alla scorsa settimana.
- Nuovi: 69630, +**28** 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*

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.