



ubuntu-it

**Newsletter Ubuntu-it**

**Numero 021 – Anno 2020**

<https://ubuntu-it.org/news/newsletter>



## Newsletter Ubuntu-it

Redattori:

- [Dario Cavedon](#)
- [Diego Prioretti](#)
- [Stefano Dall'Agata](#)
- [Alessandro Viprati](#)
- [Pietro Albini](#)
- [Luca Ciavatta](#)
- [Devid Antonio Filoni](#)
- [Daniele De Michele](#)

La Newsletter di Ubuntu-italia ha lo scopo di tenere aggiornati tutti gli utenti appassionati e non della distribuzione Ubuntu e dovrà essere gratuita e fruibile in diversi modi. Le uscite avranno cadenza settimanale e verranno pubblicate ogni Lunedì. La newsletter è aperta al contributo di tutti gli utenti che vogliono partecipare con un proprio articolo, dove questo dovrà essere inserito nella pagina [Articoli di Prova](#) e sottoposto alla valutazione dei redattori. È necessario che gli utenti seguano le raccomandazioni e le istruzioni dettagliate riportate nella pagina [Linee Guida](#). 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. La scadenza per la presentazione degli articoli da pubblicare sarà tra Sabato e Domenica, dove salvo imprevisti verranno mantenuti e pubblicati nel numero successivo. 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 maggiori informazioni:

[Newsletter Ubuntu-it](#)

## Copyright

Il presente documento e il suo contenuto è distribuito con licenza Creative Commons 4.0 di tipo "Attribuzione - Condividi allo stesso modo". È possibile, riprodurre, distribuire, comunicare al pubblico, esporre al pubblico, rappresentare, eseguire o recitare il presente documento alle seguenti condizioni:



**Attribuzione** – Devi riconoscere una menzione di paternità adeguata, fornire un link alla licenza e indicare se sono state effettuate delle modifiche. Puoi fare ciò in qualsiasi maniera ragionevole possibile, ma con modalità tali da suggerire che il licenziante avalli te o il tuo utilizzo del materiale.



**Stessa Licenza** – Se remixi, trasformi il materiale o ti basi su di esso, devi distribuire i tuoi contributi con la stessa licenza del materiale originario.

**Divieto di restrizioni aggiuntive** - Non puoi applicare termini legali o misure tecnologiche che impongano ad altri soggetti dei vincoli giuridici su quanto la licenza consente loro di fare.

Un riassunto in italiano della licenza è presente a questa [pagina](#). Per maggiori informazioni:

<http://www.creativecommons.org>

## Indirizzi

[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

## Numero 021 – Anno 2020

<b>1. Notizie da Ubuntu.....</b>	<b>2</b>
1.1 In arrivo la prima point release di Ubuntu 20.04 LTS.....	2
1.2 Canonical rilascia un nuovo aggiornamento per il kernel Linux in Ubuntu 20.04 LTS, 19.10 e 18.04 LTS.....	3
1.3 Autenticazione SSH e FIDO migliorata in Ubuntu 20.04 LTS.....	3
<b>2. Notizie dalla comunità internazionale.....</b>	<b>4</b>
2.1 Full Circle Magazine Issue #157 in inglese.....	4
<b>3. Notizie dallo Mondo.....</b>	<b>4</b>
3.1 Arriva il Raspberry Pi 4 con 8 GB di RAM.....	4
3.2 Disponibile la nuova beta a 64 bit di Raspbian.....	5
3.3 Thunderspy, la vulnerabilità che colpisce le interfacce Thunderbolt di Intel (e Apple).....	5
<b>4. Aggiornamenti e statistiche.....</b>	<b>6</b>
4.1 Aggiornamenti di sicurezza.....	6
4.2 Bug riportati.....	6
4.3 Statistiche del gruppo sviluppo.....	6
<b>5. Commenti e informazioni.....</b>	<b>7</b>
<b>6. Lavora con noi.....</b>	<b>7</b>



## Newsletter Ubuntu-it

### Numero 021 – Anno 2020

Benvenuta/o alla newsletter della **comunità italiana** di Ubuntu! Questo è il numero **21** del **2020**, riferito alla settimana che va da **lunedì 25 maggio** a **domenica 31 maggio** Per qualsiasi commento, critica o lode, contattaci attraverso la [mailing list](#) del [gruppo promozione](#).

#### 1. Notizie da Ubuntu

##### 1.1 In arrivo la prima point release di Ubuntu 20.04 LTS

Salvo eventuali problemi, il 23 Luglio 2020 sarà previsto il rilascio della prima point release di Ubuntu **20.04 LTS**. Questo primo aggiornamento non porterà grande novità, se non che raggruppa tutti gli aggiornamenti di base rilasciati dalla distribuzione da Aprile. Inoltre, sempre grazie al rilascio del nuovo punto, il 23 Luglio gli utenti che utilizzano **Ubuntu 18.04 LTS** saranno informati della disponibilità di una versione più recente di Ubuntu. Il suddetto meccanismo riguarda solo le versioni *long-term support* che oltre ad offrire 5 anni di supporto sono incentrate sulla stabilità, permettendo ad un utente di "temporeggiare" sull'avanzamento di sistema ed essere sicuro che tutti i bug individuati nella nuova release siano stati risolti. Quindi, qualora si desiderasse eseguire l'upgrade alla release **20.04 LTS**, si potrà fare senza problemi, tenendo a mente di eseguire prima dell'aggiornamento un backup dei propri dati.

Fonte:  
[omgubuntu.co.uk](http://omgubuntu.co.uk)

## 1.2 Canonical rilascia un nuovo aggiornamento per il kernel Linux in Ubuntu 20.04 LTS, 19.10 e 18.04 LTS

Per chi lavora nell'ambito della sicurezza è cosciente del fatto che, c'è una piccola probabilità che se si patcha una vulnerabilità, da qualche altra parte se ne crea una nuova. Questo è quello che è successo con l'ultimo aggiornamento rilasciato da **Canonical** (per maggiori informazioni [2020.020](#) e [2020.020](#)) che andava a risolvere delle vulnerabilità riscontrate nelle versioni del kernel linux 5.4 e 5.3 utilizzate nelle distribuzioni **Ubuntu 20.04 LTS, 19.10 e 18.04 LTS**. La regressione in questione [USN-4367-1](#), ha interessato l'implementazione del [file system Btrfs](#) del kernel Linux, causando il riavvio della macchina o ancora degli arresti anomali. Prontamente **Canonical** ha rilasciato una patch per sopperire a questo piccolo inconveniente, consigliando a tutti gli utenti di aggiornare quanto il prima le proprie distribuzioni e di ricordarsi di riavviare i computer dopo aver installato la nuova versioni del kernel Linux. Per ulteriori informazioni riguardanti le istruzioni di aggiornamento visitare la [pagina](#) sviluppata dalla **comunità Ubuntu-it**.

Fonte:  
[9to5linux.com](#)

## 1.3 Autenticazione SSH e FIDO migliorata in Ubuntu 20.04 LTS

In termini di sicurezza, un altro grande miglioramento presente in **Ubuntu 20.04 LTS (Focal Fossa)** è la possibilità di utilizzare dei dispositivi **Fast Identity Online (FIDO)** o ancora **Universal 2nd Factor (U2F)** con SSH. Questo processo di identificazione ha il duplice scopo di permettere all'utente di utilizzare un secondo fattore di autenticazione tramite dispositivo e di aumentare il livello di sicurezza della propria infrastruttura. Questa funzionalità inserita di default in Ubuntu 20.04 LTS è disponibile attraverso l'utilizzo dell'ultima versione di **OpenSSH 8.2**. I passaggi da seguire sono abbastanza semplice, perché la gestione dei file delle chiavi pubbliche e private è rimasta pressoché invariata, dove spetta agli utenti aggiungere o meno una [passphrase](#) alla chiave privata. Inoltre, una volta posizionate le chiavi è richiesto un semplice tocco del dispositivo per poter accedere. I nuovi tipi di certificati di chiave pubblica [ecdsa-sk](#) e [ed25519-sk](#) supportano questi dispositivi di autenticazione.

A questo punto attraverso dei semplici comandi, da inserire all'interno del [terminale](#), mostreremo come gli utenti potranno generare nuovi tipi di chiave e usarli per eseguire l'autenticazione. Prima tutto - necessariamente - occorre collegare il dispositivo al sistema e generare una nuova chiave e specificare uno dei nuovi tipi di chiave sopra citati. Durante questo processo, agli utenti verrà richiesto di toccare il token per confermare l'operazione, mostrando come output il seguente codice:

```
ubuntu@focal-openssh-client: ~ $ ssh-keygen -t ecdsa-sk
Generazione di coppie di chiavi ecdsa-sk pubbliche/private. Potrebbe essere
necessario toccare l'autenticatore per autorizzare la generazione della
chiave.
```

```
Inserisci file in cui salvare la chiave (/home/ubuntu/.ssh/id_ecdsa_sk):
```

```
Inserisci la passphrase (vuoto per nessuna password):
```

```
Immettere nuovamente la stessa passphrase:
```

```
La vostra identificazione è stata salvata in /home/ubuntu/.ssh/id_ecdsa_sk
```

```
La tua chiave pubblica è stata salvata in /home/ubuntu/.ssh/id_ecdsa_sk.pub
```

A questo punto è possibile confermare se sono state create le nuove chiavi pubbliche e private:

```
ubuntu@focal-openssh-client: ~ $ l.ssh/id_ecdsa_sk*
-rw----- 1 ubuntu ubuntu 610 mar 30 17:58 .ssh/id_ecdsa_sk
-rw-r--r-- 1 ubuntu ubuntu 221 mar 30 17:58 .ssh/id_ecdsa_sk.pub
```

Per concludere, l'utente dovrà copiare le chiavi con il comando `ssh-copy-id` dove verrà assicurato che la chiave pubblica sia aggiunta al file `~/.ssh/authorized_keys` sul sistema a cui desideriamo connetterci. Ora, per accedere a un dispositivo basterà eseguire il seguente comando (sempre da terminale):

```
ubuntu@focal-openssh-client:~$ ssh -i .ssh/id_ecdsa_sk 10.0.100.75
```

```
Conferma presenza utente per chiave ECDSA-SK
(...)
Benvenuto in Ubuntu Focal Fossa (ramo di sviluppo)
(GNU/Linux 5.4.0-18-generic x86_64)
(...)
Ultimo accesso: Lun 30 Mar 20:29:05 2020 dal 10.0.100.1
ubuntu@focal-openssh-server: ~ $
```

dove verrà visualizzato un messaggio per confermare la presenza di un nuovo utente. Per concludere l'autenticazione l'utente dovrà toccare il proprio token, completando così l'iter di sicurezza.

Fonte:  
[ubuntu.com](https://ubuntu.com)

## 2. Notizie dalla comunità internazionale

### 2.1 Full Circle Magazine Issue #157 in inglese

È stato pubblicato sul sito internazionale di [Full Circle Magazine](https://www.fullcirclemagazine.org/), il numero 157 in Inglese. In questo numero troviamo:

- Comanda e Conquista
- How-To: Python, LivePatch, e Rawtherapee
- Grafica: Inkscape
- Grafica: Krita per Vecchie Foto
- Tutti i Giorni Ubuntu: Turbogfx 16
- Ubports Touch : OTA-12
- Recensione: Ubuntu, Lubuntu e Budgie 20.04
- Giochi Ubuntu: Eagle Island

... e molto altro ancora.

È possibile scaricare la rivista da [questa pagina](#).

## 3. Notizie dallo Mondo

### 3.1 Arriva il Raspberry Pi 4 con 8 GB di RAM

A breve la tanto amata versione 4 della scheda Raspberry Pi compirà un anno e per portare una nuova boccata d'aria all'interno della comunità, la **Raspberry Pi Foundation**

ha annunciato la disponibilità della sua scheda Raspberry Pi 4 con 8 GB di RAM a un modico prezzo di 75 dollari. Non solo perché al contempo è stato ridotto anche il prezzo della variante da 2 GB da 45 a 35 dollari. Sebbene comunque la nuova variante costi di più, offre delle novità importanti, infatti il [chip BCM2711](#) di Broadcom permette, grazie all'utilizzo di un processore ARM Quad-Core Cortex-A72 a 64 bit, di gestire fino a 16GB di LPDDR4 SDRAM. Risulta quindi evidente come la versione da 8GB diventi un nuovo capo saldo per tutti quegli sviluppatori che hanno necessita di poter navigare nel web senza sentirsi limitati nel numero di pagine da aprire o ancora nel compilare dei codici che richiedono un enorme capacità di calcolo. Lato software sono stati fatti notevoli miglioramenti con la ricompilazione in versione beta del pacchetto a 64 bit di **Raspbian OS** in grado di gestire blocchi di memoria superiori a 3GB, cosa precedentemente non possibile dato questa è una limitazione che grava sulle architetture a 32 bit. Mentre lato hardware invece, oltre l'implementazione di 8 GB di RAM, sono state fatte delle variazioni riguardo l'alimentazione della scheda per permetterle di gestire questo incremento di memoria. Quindi, se già da tempo stavi pensando di acquistare una scheda **Raspberry Pi**, beh sappi che è giunta l'ora, in quanto il nuovo modello è già disponibile negli [store dei rivenditori](#) approvati da Raspberry.

Fonte:

[raspberrypi.org](http://raspberrypi.org)

[fossbytes.com](http://fossbytes.com)

[9to5linux.com](http://9to5linux.com)

### 3.2 Disponibile la nuova beta a 64 bit di Raspbian

Come scritto nell'articolo precedente, con il lancio della nuova scheda Raspberry Pi 4 da 8 GB, la **Raspberry Pi Foundation** ha svelato anche la versione beta a 64 bit del proprio sistema operativo [Raspbian](#). Il sistema è basato sulla famosa distribuzione Linux **Debian**, e utilizza un ambiente grafico modificato LXDE chiamato [PIXEL](#). Però, per rendere Raspbian più appetibile e di conseguenza dare il via alla sua adozione all'interno della comunità, che vede aumentare esponenzialmente i suoi utenti con il passare del tempo, la Raspberry Pi Foundation ha deciso di cambiare il nome della loro distribuzione GNU/Linux in **Raspberry Pi OS**. Questo cambiamento ha una duplice valenza, perché fino ad ora Raspbian era disponibile solo come immagine a 32 bit per tutti i modelli Raspberry Pi supportati, ma con l'introduzione della nuova scheda si è deciso di adottare una variante a 64 bit, per poter permettere agli sviluppatori di usufruire dell'intera memoria qualora si utilizzi la propria scheda come desktop PC o come server e mantenere alti i carichi di lavoro. Al momento **Raspberry Pi Foundation** consiglia a tutti gli utenti di continuare ad usare la versione 32 bit di Raspberry Pi OS dato che la release a 64 bit è ancora in versione beta. Tuttavia, in alternativa si possono utilizzare sistemi a 64 bit come **Ubuntu**. Se anche tu, vuoi testare l'ultima versione del sistema operativo Raspberry Pi scaricare l'immagine dal [seguente link](#).

Fonte:

[9to5linux.com](http://9to5linux.com)

### 3.3 Thunderspy, la vulnerabilità che colpisce le interfacce Thunderbolt di Intel (e Apple)

Questa volta a pagarne le conseguenze non è una famiglia di processori, come con la comparsa di **Meltdown**, ma una svariata quantità di dispositivi che implementano questo standard di comunicazione, che prende il nome di [Thunderbolt](#). Questa tecnologia è stata sviluppata da Intel, nel lontano 2001 con la collaborazione di Apple, che permette, attraverso una semplice interfaccia grafica, il collegamento di diversi dispositivi multimediali quali fotocamere digitali, schermi etc. Queste falle - per la precisione 7 -

vengono raggruppate sotto la denominazione di **Thunderspy** e, sono state messe alla luce da un ricercatore di sicurezza olandese Björn Ruytenberg, che pone in evidenza il fatto che una volta che l'attacco è avvenuto con successo, esso sia completamente invisibile a qualunque tipo di controllo o ispezione, permettendo di prendere il pieno possesso del dispositivo. Da notare però che, per quanto non esistano soluzioni a riguardo, visto che tutti i portatili che implementano una porta **Thunderbolt 3** sono vulnerabili, l'attacco da eseguire è assai complicato, perché occorre che il malvivente oltre ad avere un accesso fisico alla macchina, debba smontare la parte inferiore del notebook per poi arrivare alla scheda madre, dove verrà collegato un dispositivo alla porta Thunderbolt (che verrà utilizzato successivamente per riprogrammare il firmware) per poi rimontare la parte posteriore della macchina. Questa vulnerabilità segna un varco all'interno della sicurezza informatica, perché tenendo conto delle complicazione appena dette, l'intrusione sarebbe completamente invisibile permettendo a chi che sia, di fare una copia dell'intero disco, saltando i passaggi di cifratura che si hanno quando si accende la macchina. Parrebbe fantascienza, invece è pure realtà.

Al momento milioni di dispositivi prodotti prima del 2019 sarebbero vulnerabili, mentre per quelli prodotti recentemente **Intel** ha introdotto un sistema chiamato [Kernel Direct Memory Access Protection](#) che né limita l'attacco. Per concludere, il ricercatore olandese ha inoltre sviluppato una [pagina web](#) molto dettagliata, dove oltre a spiegare con particolare minuzia come funziona la vulnerabilità, mette a disposizione gratuitamente per tutti gli utenti un programma che permette di verificare la propria vulnerabilità.

Fonte:  
[theverge.com](https://theverge.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: 133737, **+150** rispetto alla scorsa settimana.
- Critici: 366, **-1** rispetto alla scorsa settimana.
- Nuovi: 65701, **+118** 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.

### 4.3 Statistiche del gruppo sviluppo

Segue la lista dei pacchetti realizzati dal [Gruppo Sviluppo](#) della comunità italiana nell'ultima settimana:

*Mattia Rizzolo*

- [libsndfile 1.0.28-8](#), per Debian unstable

Se si vuole contribuire allo sviluppo di Ubuntu correggendo bug, aggiornando i pacchetti nei repository, ecc... il gruppo sviluppo è sempre alla ricerca di nuovi volontari.



## 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](#)
- [Stefano Dall'Agata](#)

Ha realizzato il pdf:

- [Daniele De Michele](#)

## 6. Lavora con noi

La newsletter è aperta al contributo di tutti coloro che vogliono partecipare con un proprio articolo. Questo dovrà essere inserito nella pagina [Articoli di Prova](#) e sottoposto alla valutazione dei redattori prima della scadenza che avviene tra il Sabato e la Domenica. L'autore dell'articolo troverà tutte le raccomandazioni e istruzioni dettagliate all'interno della pagina [Linee Guida](#), dove gli articoli potranno trattare qualsiasi argomento che riguarda le principali novità di Ubuntu e sulla comunità internazionale, tutte le informazioni sulle attività della comunità italiana, le notizie sul software libero dall'Italia e dal mondo ecc. Per chiunque fosse interessato a collaborare con la newsletter di Ubuntu-it a qualsiasi titolo quale redattore, editore, grafico, può scrivere alla [mailing list](#) del [gruppo promozione](#) oppure sul canale IRC: #ubuntu-it-promo.

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"*