
FREE CIRCLE

Fidarsi è bene.
Verificare è meglio.

Lorenzo Faletra · Parrot Security · Linux Day Palermo 2026

Le vulnerabilità hanno un nome.

Chi le ha trovate. Quanto ci è voluto per chiuderle.

The Heartbleed Bug

This bug was independently discovered by a team of security engineers (Riku, Antti and Matti) at Codenomicon and Neel Mehta of Google Security, who first reported it to the OpenSSL team. Codenomicon team found heartbleed bug while improving the SafeGuard feature in Codenomicon's Defensics security testing tools and reported this bug to the NCSC-FI for vulnerability coordination and reporting to OpenSSL team.

Trovata due volte.

heartbleed.com (evidenziazione aggiunta)

6 giorni

dalla segnalazione alla versione corretta

ma il bug era nel codice da 2 anni

Shellshock · 2014

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.

Una persona. Una mail.

nvd.nist.gov/vuln/detail/CVE-2014-6271 (evidenziazione aggiunta)

12 giorni

dalla segnalazione alla patch

ma il bug era in bash dal 1989

The Dirty Pipe Vulnerability

It all started a year ago with a support ticket about corrupt files. A customer complained that the access logs they downloaded could not be decompressed. And indeed, there was a corrupt log file on one of the log servers; it could be decompressed, but `gzip` reported a CRC error. I could not explain why it was corrupt, but I assumed the nightly split process had crashed and left a corrupt file behind. I fixed the file's CRC manually, closed the ticket, and soon forgot about the problem.

Un ticket di assistenza.

dirtypipe.cm4all.com, Max Kellermann (evidenziazione aggiunta)

3 giorni

dalla segnalazione ai kernel corretti

Android: il giorno dopo

Remote Unauthenticated Code Execution Vulnerability in OpenSSH Server (regreSSHion)

Un’azienda di sicurezza.

il bug del 2006, tornato nel 2020

OpenSSH 9.8/9.8p1 (2024-07-01)

OpenSSH 9.8 was released on 2024-07-01. It is available from the

and one minor.

1) Race condition in sshd(8)

A critical vulnerability in sshd(8) was present in Portable OpenSSH versions between 8.5p1 and 9.7p1 (inclusive) that may allow arbitrary code execution with root privileges.

Annuncio e patch:
lo stesso giorno.

Attacking UNIX Systems via CUPS, Part I

BY **Simone Margaritelli** — 26 Sep 2024 — **cups**, **cups-browsed**, **printer**, **printing**, **unix**, **hacking**, **rce**, **disclosure**, **exploit**, **ipp**, **udp**, **responsible disclosure**, **vulnerability research**, **linux security**, **print services**, **unauthenticated access**, **cve**, **CVE-2024-CVE-2024-47076**, **CVE-2024-47175**, **CVE-2024-47177**

Follow @evilsocket

Un portatile nuovo.

UDP 0.0.0.0:631, in ascolto su tutte le interfacce

21 giorni

di discussioni con i manutentori

Non sempre è una favola.

```
Message-ID: <20240329155126.kjjfduxw2yrlxgzm@awork3.anarazel.de>
Date: Fri, 29 Mar 2024 08:51:26 -0700
From: Andres Freund <andres@...razel.de>
To: oss-security@...ts.openwall.com
Subject: backdoor in upstream xz/liblzma leading to ssh server compromise

Hi,

After observing a few odd symptoms around liblzma (part of the xz package) on
Debian sid installations over the last weeks (logins with ssh taking a lot of
CPU, valgrind errors) I figured out the answer:

The upstream xz repository and the xz tarballs have been backdoored.
```

```
== Observing Impact on openssh server ==

With the backdoored liblzma installed, logins via ssh become a lot slower.

time ssh nonexistant@...alhost

before:
nonexistant@...alhost: Permission denied (publickey).

before:
real    0m0.299s
user    0m0.202s
sys     0m0.006s

after:
nonexistant@...alhost: Permission denied (publickey).

real    0m0.807s
user    0m0.202s
sys     0m0.006s
```

Mezzo secondo.

Chi l’ha trovata
lavorava per Microsoft.

With a library this widely used, the severity of this vulnerability poses a threat to the entire Linux ecosystem. Luckily, this issue was caught quickly so the impact was significantly less than it could have been. It has already been patched in Debian, and therefore, Kali Linux.

Lo stesso giorno.

e le versioni stabili non erano mai state toccate

kali.org/blog/about-the-xz-backdoor, 29 marzo 2024 (evidenziazione aggiunta)

Heartbleed
Google + Codenomicon
6 giorni

Shellshock
Stéphane Chazelas
12 giorni

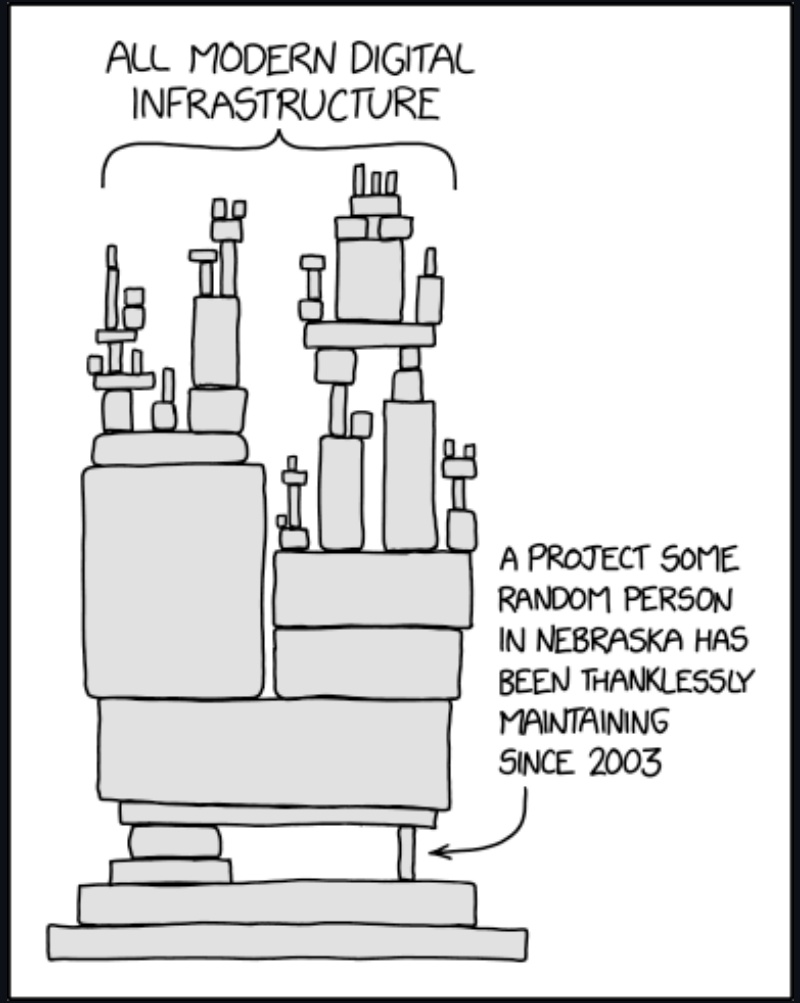
Dirty Pipe
Max Kellermann · IONOS
3 giorni

regreSSHion
Qualys
all’annuncio

CUPS
Simone Margaritelli
21 giorni

xz
Andres Freund · Microsoft
lo stesso giorno

Community e aziende.
Stesso tavolo.



xkcd.com/2347 · Randall Munroe · CC BY-NC 2.5

$2.000

di donazioni l’anno.

OpenSSL, prima di Heartbleed (2014)

Le chiavi dell’albergo.


Applicazioni
browser · terminale · servizi (user space)
↓ system call ↓
Kernel
decide chi può fare cosa
↓
Hardware

Due mondi.



Anche root ha un regolamento.

Linux Security Modules

SELinux
AppArmor

Marzo 2001

La NSA presenta SELinux al Kernel Summit.

Linus: fatene un framework.

Il codice della NSA
è nel vostro kernel.

Ed è una buona notizia.

SELinux

Etichette.

Fedora · RHEL · Android · openSUSE

AppArmor

Percorsi.

Ubuntu · Debian

default per le nuove installazioni · openSUSE Tumbleweed: SELinux dal 2025

```
# setenforce 0
```

...e da qualche parte Dan Walsh piange.


Un container
non esiste.

namespaces → cosa vedi

seccomp → cosa puoi fare

cgroups → quanto consumi

OverlayFS → su cosa poggi

reti virtuali → con chi parli

= un container.

Namespaces

```
$ ls /proc/self/ns
```

```
cgroup   ipc   mnt   net
pid   time   user   uts
```

Cosa vedi.

Seccomp

Un italiano. seccomp. Andrea Arcangeli, 2005.

Cosa puoi fare.

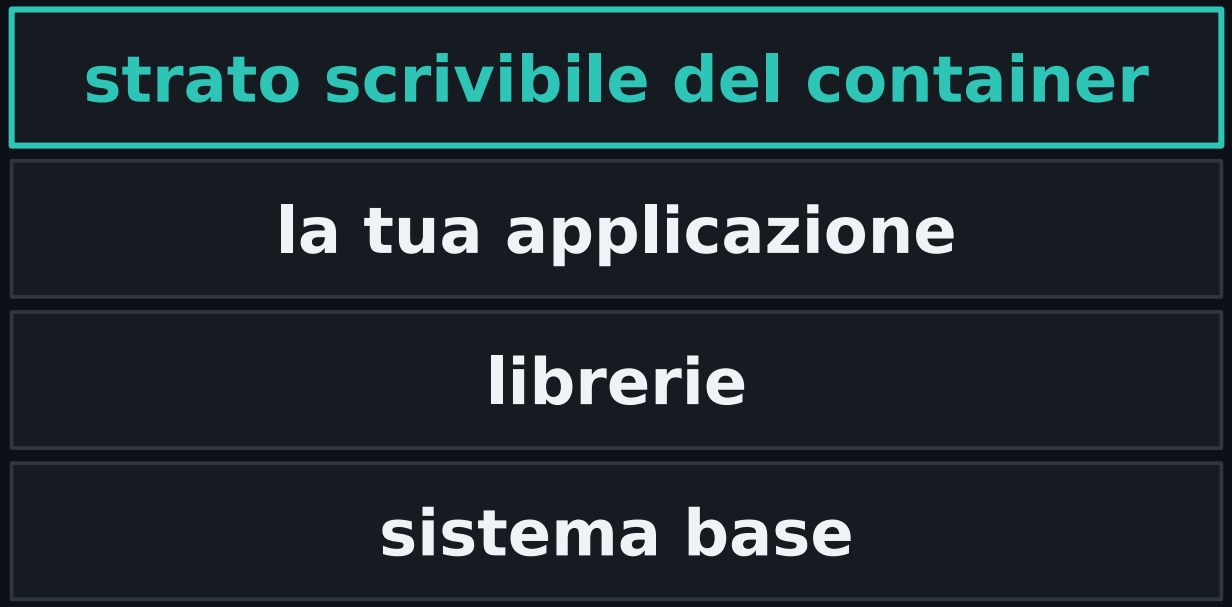
Cgroups

Quanto consumi.

in Linux dal 2008 Google, 2006.



Un kernel, mille mondi.



Strati.

OverlayFS · nel kernel da Linux 3.18, 2014

```
$ whoami
lorenzo
$ unshare --user --map-root-user \
      --pid --fork --mount-proc bash
# whoami
root
# ps -e
(solo bash e ps)
```

Un container in una riga.
Senza Docker.



— Funziona sulla mia macchina.

— Allora spediremo la tua macchina.

...ed è così che è nato Docker.

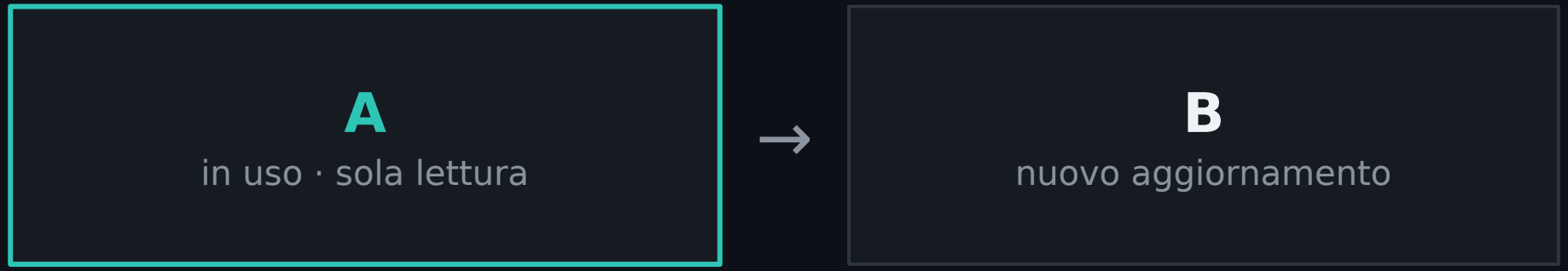
Container e orchestrazione

Docker
Podman
Kubernetes

Sandbox per le applicazioni

bubblewrap

firejail



riavvio → B. Qualcosa va storto? **Torni ad A.**

Tutto o niente.

Ce l’avete in mano.



Steam Deck, foto Liam Dawe/GamingOnLinux, CC BY-SA 4.0, Wikimedia Commons (sfondo aggiunto)

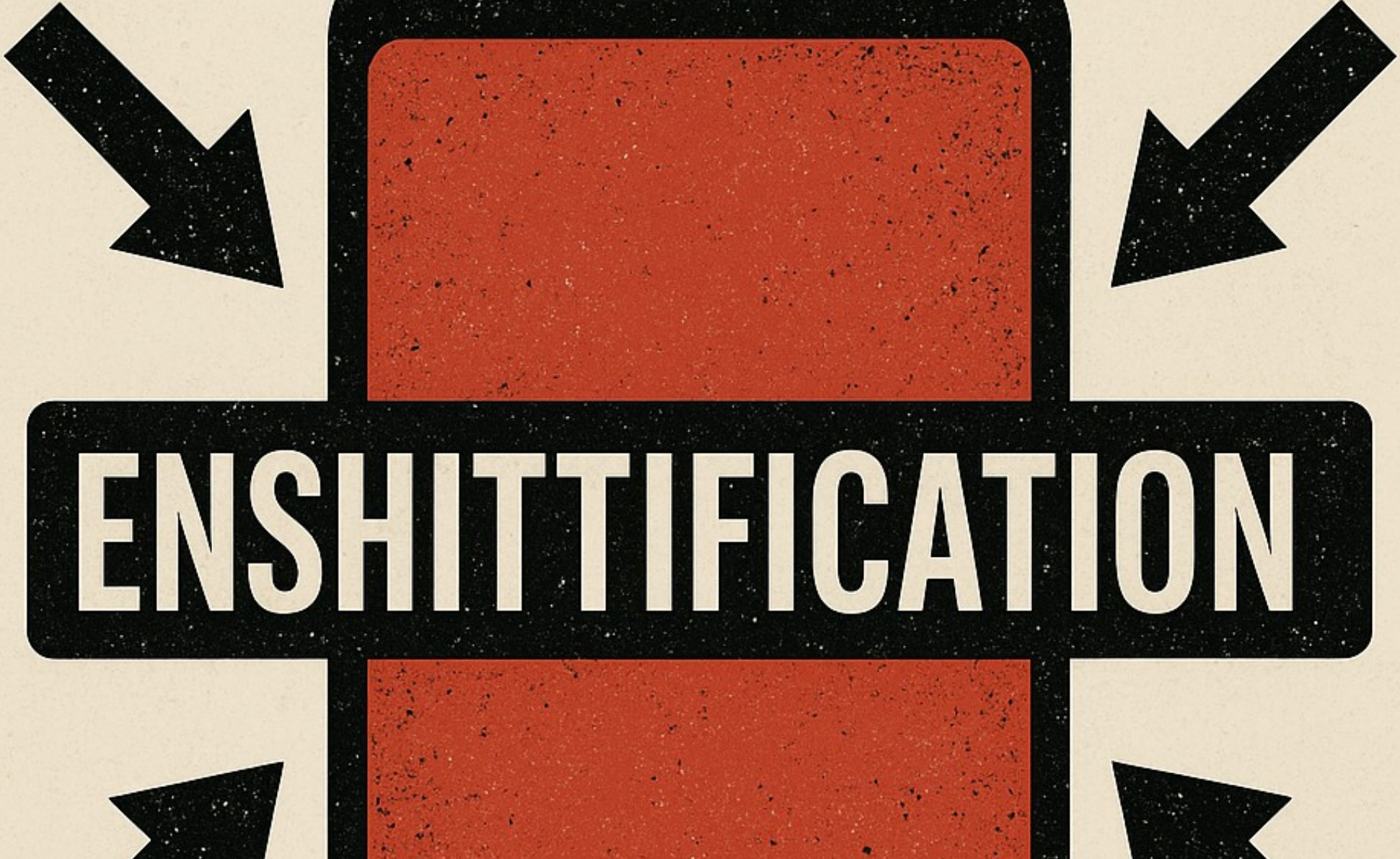
The Fedora website currently uses the term "Immutable Desktops" to regroup all desktop, `rpm-ostree` based Fedora variants. The term "immutable" is confusing to users, has been the source of many confusion and does not accurately reflect the advantages of those variants.

Atomiche, non immutabili.

fedoraproject.org/wiki/Changes/AtomicDesktops (evidenziazione aggiunta)

Nel frattempo, a Redmond.


U.S.
CYBERSECURITY
STOP
©2015 6-9 Dist. by Wash. Post Writers Group


ENSHITTIFICATION

Il secondo martedì del mese.

...e il mercoledì, gli exploit.

Patch Tuesday, dall’ottobre 2003

```
msf > use exploit/windows/smb/ms08_067_netapi
```

Microsoft Security Bulletin MS08-067 - Critical

Published: October 23, 2008

Corretta. Fuori ciclo.

learn.microsoft.com, bollettino MS08-067 (evidenziazione aggiunta)

E allora perché
ha funzionato per anni?

Perché le macchine
non si aggiornavano.

```
msf > use exploit/windows/smb/ms17_010_eternalblue
```

MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

Un exploit della NSA.
Tenuto segreto per 5 anni.

patch: 14 marzo 2017 · pubblicato dagli Shadow Brokers: 14 aprile 2017

rapid7.com, modulo Metasploit ms17_010_eternalblue

Marzo 2017: la patch.
Maggio 2017: WannaCry.

Today many of our customers around the world and the critical systems they depend on were victims of malicious “WannaCrypt” software. Seeing businesses and individuals affected by cyberattacks, such as the ones reported today, was painful. Microsoft worked throughout the day to ensure we understood the attack and were taking all possible actions to protect our customers. This blog spells out the steps every individual and business should take to stay protected. Additionally, we are taking the highly unusual step of providing a security update for all customers to protect Windows platforms that are in custom support only, including Windows XP, Windows 8, and Windows Server 2003. Customers running Windows 10 were not targeted by the attack today.

Microsoft MSRC, 13 maggio 2017 (evidenziazione aggiunta)

Finally, this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action.

Come farsi rubare dei missili Tomahawk.

blogs.microsoft.com, Brad Smith, 14 maggio 2017 (evidenziazione aggiunta)

2 mesi

Beaumont said other researchers on April 12, 2022 told Microsoft about active exploitation of the MSDT flaw, but Microsoft closed the ticket saying it wasn't a security issue. Microsoft finally issued a CVE for the problem on May 30, the same day it released recommendations on how to mitigate the threat from the vulnerability.

Follina, 2022: «non è un problema di sicurezza»

krebsonsecurity.com, giugno 2022 (evidenziazione aggiunta)

2001 Ballmer: 'Linux is a cancer'

2014 Redmond top man Satya Nadella: 'Microsoft LOVES Linux'

2024 Prioritizing security above all else

Due svolte in vent’anni.

theregister.com (2001, 2014) · blogs.microsoft.com (2024)

“Complexity is the worst enemy of security.”

Bruce Schneier, 2012

BS: I’m sure that this isn’t the answer that many would want to hear but yes this is the reality today. I’m sure that out there somewhere is a point where the complexity slows down and we find a way to gain back some ground. But it’s hard to envisage as there is so much change and it’s happening so fast that every new thing brings added complexity. And complexity is the worst enemy of security.

Murphy’s law in the Mass Surveillance Age



Murphy’s law in the Mass Surveillance Age

threatpost

Cynet: An Autonomous Security Platform for Any Size Orga

Linux Ke

WhatsApp Zero-Day Exploited in Targeted Spyware Attacks





Author:
Lindsey O'Donnell

May 14, 2019
/ 8:58 am

5 minute read

Skip to:

WhatsApp has patched a vulnerability that allowed attackers to install spyware on victims’ phones.

UPDATE

WhatsApp is urging users to update as soon as possible, after a zero-day vulnerability found in its messaging platform was exploited by attackers who were able to inject spyware onto victims’ phones in targeted campaigns.

Paragon Spyware Used in WhatsApp Hacking Scandal

READ MORE

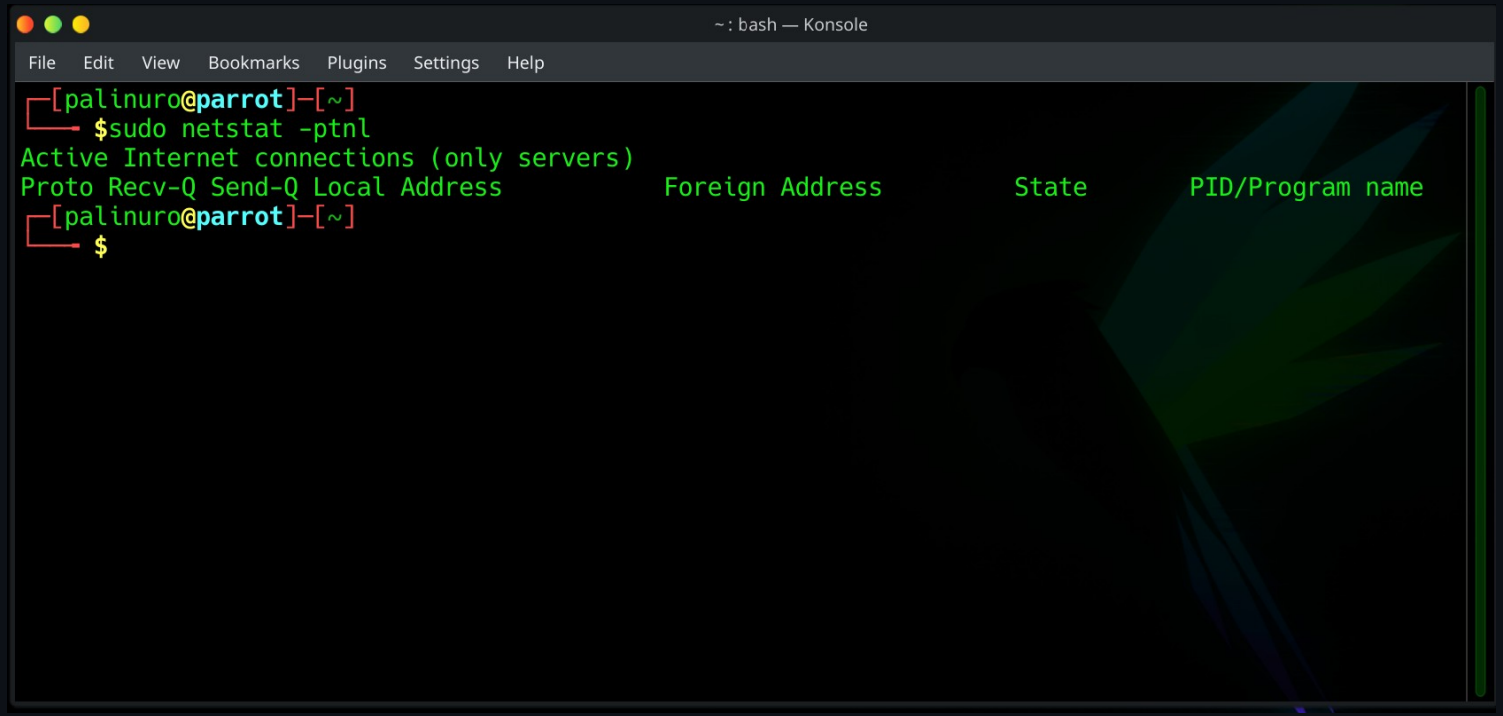



Vista
LO SPECIALE
ANSA

40 milioni

di righe di codice nel kernel Linux (6.13, 2025)

Linux non è semplice.



Ma ti lascia esserlo.

Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users

- Use an ad blocking extension when performing internet searches. Most internet browsers allow a user to add extensions, including extensions that block advertisements. These ad blockers can be turned on and off within a browser to permit advertisements on certain websites while blocking advertisements on others.

Lo dice l’FBI.

ic3.gov/PSA/2022/PSA221221, 21 dicembre 2022





NoScript

uBlock Origin

loghi dai repository ufficiali: hackademix/noscript · gorhill/uBlock


European
Parliament
Europäisches
Parlament



2001 «Linux is a cancer»

2014 «Microsoft loves Linux»

2024 un ingegnere Microsoft salva Linux

Ha vinto il modello in cui chiunque può guardare.

```
== Analyzing the injected code ==

I am *not* a security researcher, nor a reverse engineer.  There's lots of
stuff I have not analyzed and most of what I observed is purely from
observation rather than exhaustively analyzing the backdoor code.
```

I molti occhi siete voi.

oss-security, 29 marzo 2024 (evidenziazione aggiunta)

Fidarsi è bene.
Verificare è meglio.



Read-only. Di default.

→ Antonio Broi · Tsurugi Linux



Me

palinuro@parrotsec.org
palinuro@linux.it

www.palinuro.me



© Lorenzo Faletra - 2026 – Creative Commons 3.0 BY-SA