DIRTY PIPE VULNERABILTY

CVE:

2022-0847

CVSS-Score:

7.8 (high)

Abstract:

Dirty Pipe vulnerability is a Linux kernel vulnerability that allows the ability of non-privileged users to overwrite read-only files. The vulnerability is due to an uninitialized “pipe_buffer.flags” variable, which overwrites any file contents in the page cache even if the file is not permitted to be written, immutable, or on a read-only mount, including CD-ROM mounts.

The page cache is always writable by the kernel and writing to a pipe never checks any permissions.

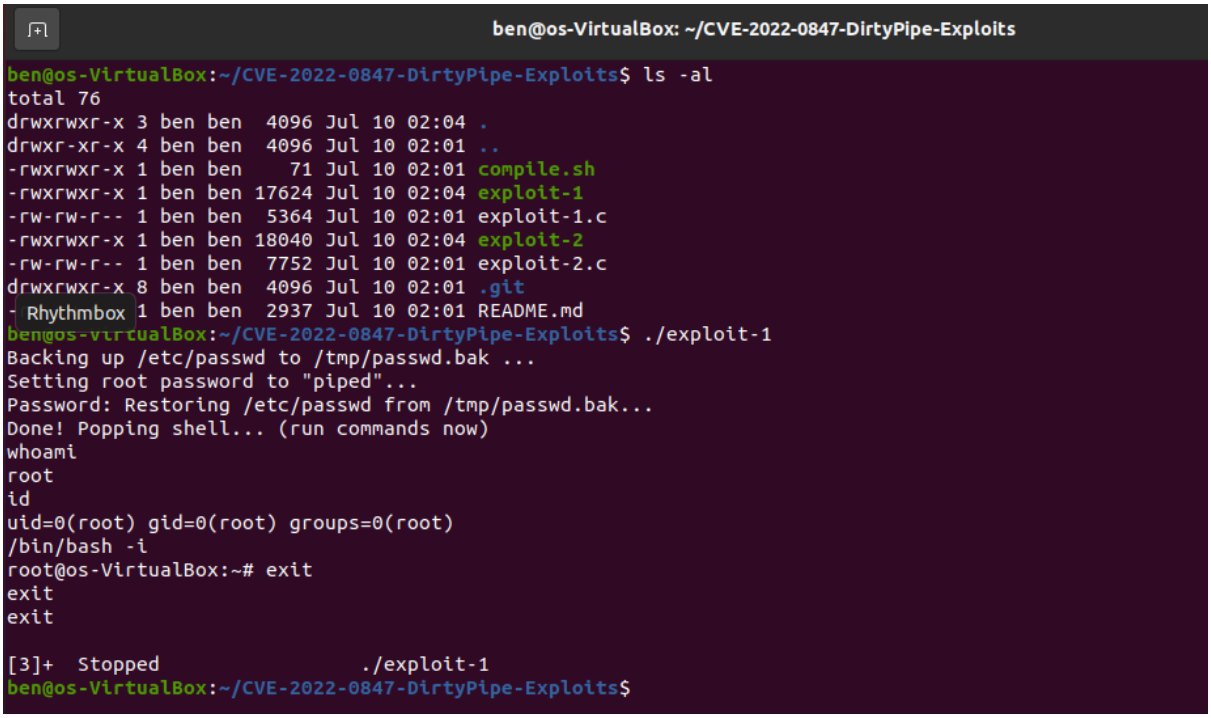
This enables attackers to perform privilege escalation by overwriting data in arbitrary read-only files and injecting code from unprivileged processes to privileged processes. This can make Linux and Android systems vulnerable to a multitude of malware and other exploits, including ransomware.

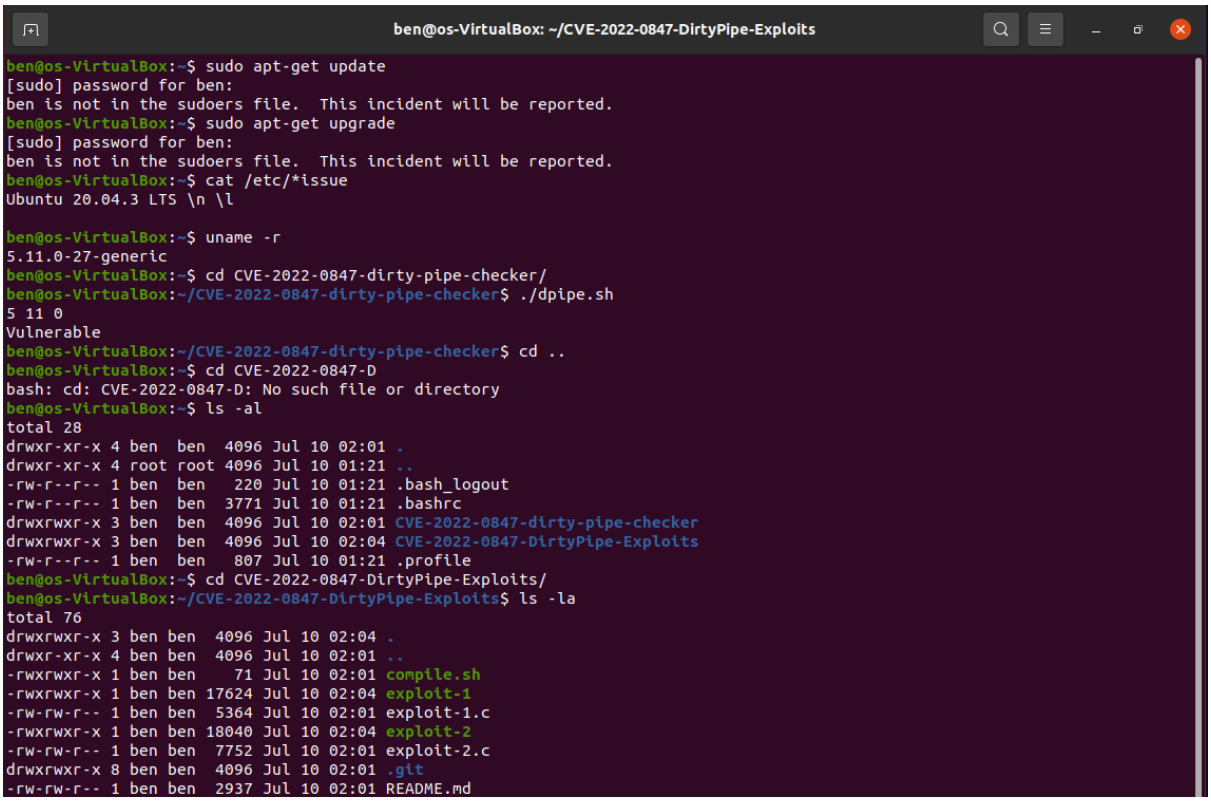
Kernel Version Affected by it

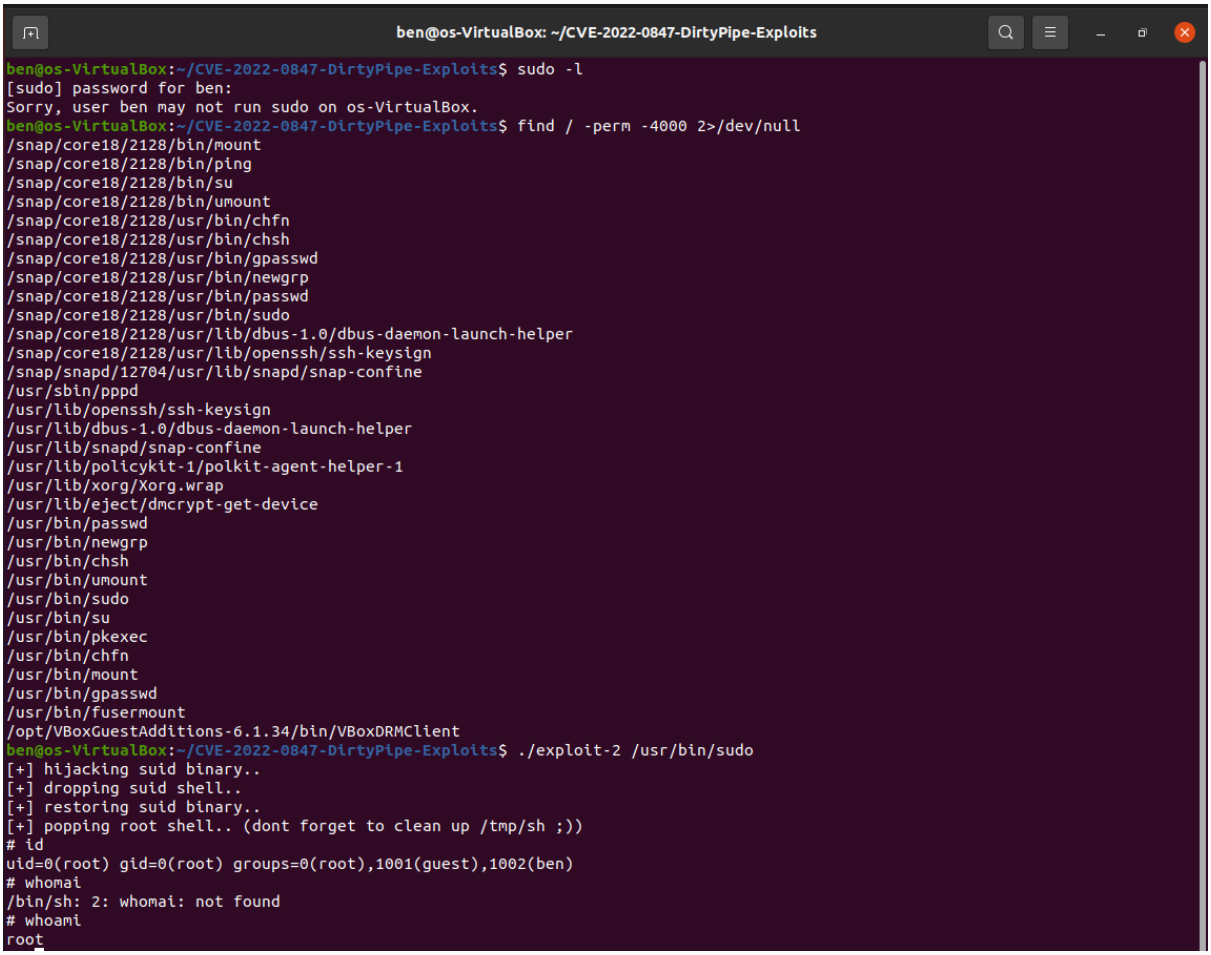
It affects the Linux kernels from 5.8 through any version before 5.16.11, 5.15.25 and 5.10.102.

This includes a multitude of devices running Android 12 and Linux.

Proof Of concept







Mitigations

- Apply all relevant security updates once they are available. To patch CVE-2022-0847, update your Linux systems to versions 5.16.11, 5.15.25 and 5.10.102 or newer.
- Use a security solution that provides patch management and endpoint protection, such as Kaspersky Endpoint Security for Linux.
- Use the latest Threat Intelligence information to stay aware of actual TTPs used by threat actors.

LABS

https://tryhackme.com/room/dirtypipe

REFERENCE

https://github.com/AlexisAhmed/CVE-2022-0847-DirtyPipe-Exploits

https://dirtypipe.cm4all.com/

https://securelist.com/cve-2022-0847-aka-dirty-pipe-vulnerability-in-linux-kernel/106088/