Summary

On March 7th, a security researcher disclosed the Dirty Pipe vulnerability affecting Linux Kernel 5.8 and later versions. The vulnerability is tracked as CVE-2022-0847 and allows a non-privileged user to inject and overwrite data in read-only files including SUID processes that run as root [1].

As per the researcher, the vulnerability is similar to CVE-2016-5195 Dirty Cow, but it is even easier to exploit.

Technical Details

A flaw was found in the way the flags member of the new pipe buffer structure lacked proper initialisation in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read-only files and, as such, escalate their privileges on the system [3].

Multiple variants of the exploit were published by the security researchers to gain root privileges by patching /usr/bin/su [4] or by overwriting /etc/passwd leading ultimately to a root shell [5].

Affected Products

This critical vulnerability affects Linux Kernel 5.8 and later versions, including Android devices.

Recommendations

The vulnerability was fixed in Linux 5.16.11, 5.15.25 and 5.10.102 [2].

Linux users with an affected kernel version (>=5.8) should apply the patches as soon as they are available.
Mitigations

Currently there is no mitigation available and SELinux does not mitigate this flaw.

References

[1] https://dirtypipe.cm4all.com/
[5] https://twitter.com/phithon_xg/status/1500902906916081666?s=20&t=n9tJBhuTd4fm-bz43s2HQ