Hive Pro

THREAT ADVISORY

Dirty Pipe: A privilege escalation vulnerability in Linux Kernel

TA2022049

Threat Level RED

Publish Date – March 8, 2022

A vulnerability in the Linux kernel existed since version 5.8 and allows overwriting data in arbitrary read-only files. Because unprivileged processes can inject code into root processes, this results in privilege escalation. It has been named Dirty Pipe by the researcher.

It is a local privilege escalation vulnerability assigned CVE-2022-0847. This bug is due to a lack of proper initialization in the Linux kernel's 'copy_page_to_iter_pipe' and 'push_pipe' functions. An attacker could use this issue to write to pages in the page cache that are backed up by read-only files, escalating their privileges on the system.

Attackers with read permissions could use the following steps to exploit this bug:

1. Create a pipe.
2. Fill the pipe with arbitrary data
3. Drain the pipe
4. Splice data from the target file into the pipe from just before the target offset.
5. Write arbitrary data into the pipe

A public POC of this issue is available. So, organizations should upgrade to Linux kernel version 5.16.11, 5.15.25 and 5.10.102 to eliminate the risk.

Potential MITRE ATT&CK TTPs are:
TA0004: Privilege Escalation
T1068: Exploitation for Privilege Escalation

Vulnerability Detail

CVE ID	Affected Product	Vulnerability Name	CWE ID
CVE-2022-0847	Linux Kernel 5.8 and later versions	Linux Kernel privilege escalation vulnerability	CWE-269

Patch Link

https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/snapshot/linux-9d2231c5d74e13b2a0546fee6737ee4446017903.tar.gz

References

https://dirtypipe.cm4all.com/