Incidents

CVE-2022-0847 aka Dirty Pipe vulnerability in Linux kernel

Incidents

14 Mar 2022

1 minute read

Table of Contents

Authors

- Expert AMR

Last week, security researcher Max Kellermann discovered a high severity vulnerability in the Linux kernel, which was assigned the designation CVE-2022-0847. It affects the Linux kernels from 5.8 through any version before 5.16.11, 5.15.25 and 5.10.102, and can be used for local privilege escalation. The vulnerability resides in the pipe tool, which is used for unidirectional communication between processes, so the researcher called it “Dirty Pipe”. Although the flaw is fixed in the latest Linux kernel versions, and, according to our data, there is no mass exploitation of this vulnerability at the moment, a detailed description and a working POC are available online, which increases the risk of this vulnerability being exploited by attackers.

Kaspersky products protect against attacks leveraging the Dirty Pipe vulnerability. The detection verdicts are:

- HEUR:Exploit.Linux.CVE-2022-0847.a
- HEUR:Exploit.Linux.CVE-2022-0847.b
- HEUR:Exploit.Linux.CVE-2022-0847.c
- HEUR:Exploit.Linux.CVE-2022-0847.gen

Dirty Pipe technical details

An unprivileged local user could use the Dirty Pipe flaw to write to pages in the page cache backed by read-only files and as such, escalate their privileges on the system. This vulnerability happens due to usage of partially uninitialized memory of the pipe buffer structure during its construction. A lack of zero initialization of the new structure’s member results in a stale value of flags, which can be abused by an attacker to gain write access to pages in the cache even if they originally were marked with a read-only attribute.

There are plenty of ways for attackers to gain the root privileges using this vulnerability, such as unauthorized creation of new cron jobs, SUID binary hijacking, /etc/passwd modification, and so on.

A working version of the Dirty Pipe exploit is already available on various security-related sites and repositories, so it can be used by attackers ITW.

Dirty Pipe mitigations

To ensure that your corporate infrastructure is protected against this and similar threats:

- 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.

IOCs (MD5 hashes of CVE-2022-0847 exploits)

ebc8f0556e031a0b1180cfdfe6bf6e03 c3662a101db6bd9edec35767c7b85741

- Linux
- Malware Technologies
- Vulnerabilities
- Vulnerabilities and exploits

Authors

- Expert AMR