Vulnerabilities 2022

Linux Kernel

CVE	In	Module	Type	Exploit Available
CVE-2021-4034	pkexec	Polkit	BOF	https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034
CVE-2022-0185	Linux Kernel	fs_context.c	Heap BOF	https://sysdig.com/blog/cve-2022-0185-container-escape/
CVE-2021-44142	Samba	Time Machine	Type Confusion	https://www.zerodayinitiative.com/blog/2022/2/1/cve-2021-44142-details-on-a-samba-code-execution-bug-demonstrated-at-pwn2own-austin
CVE-2021-26708	Linux Kernel	Socket	Race Condition	https://a13xp0p0v.github.io/2021/02/09/CVE-2021-26708.html
CVE-2022-0847	Linux Kernel	Dirty pipe	Race Condition	https://sysdig.com/blog/cve-2022-0847-dirty-pipe-sysdig/
CVE-2021-23134	Linux Kernel	NFC	UAF	https://ruia-ruia.github.io/NFC-UAF/
CVE-2022-27666	Linux Kernel	ESP6 module	BOF	https://etenal.me/archives/1825
CVE-2022-0435	Linux Kernel	TPIC Module	Stack BOF	https://www.openwall.com/lists/oss-security/2022/02/10/1
CVE-2022-1015 CVE-2022-1016	Linux Kernel	Netfilter	OOB Leak	https://blog.dbouman.nl/2022/04/02/How-The-Tables-Have-Turned-CVE-2022-1015-1016/

More vulns

CVE-2022-0646 ?
CVE-2022-0492 https://unit42.paloaltonetworks.com/cve-2022-0492-cgroups/