

## Forum: [Hack Forums](#)

Thread: [IonStack part II: GhostLock, a stack-UAF that has existed in ALL Linux distributions](#)

**MadScientist** - July 8, 2026, 10:58 pm

GhostLock (CVE-2026-43499) is a Linux kernel vulnerability found by VEGA that exists in every major distribution since 2011. Triggering the bug does not require any special kernel config or privilege. By turning it into a 97% stable privilege escalation and container escape, Google has rewarded us \$92,337 in kernelCTF. This writeup covers the technical details of the exploit.

### Vulnerability Summary

GhostLock (CVE-2026-43499) lets an unprivileged local attacker:

- Get a dangling kernel pointer to kernel stack memory with only regular threading syscalls.
- Write a pointer to an almost arbitrary address.
- Hijack a function table to get control flow hijack and eventually get root access.

GhostLock was introduced in Linux 2.6.39 and fixed in Linux 7.1. It has existed in the Linux kernel for more than 15 years. Every Linux distribution without the patch is affected and should consider upgrading to the latest LTS version.

Read More - <https://nebusec.ai/research/ionstack-part-2/>