Subject: Urgent: GhostLock (CVE-2026-43499) on OpenVZ 7 Where is the patch for WebPros / SolusVM users?
Posted by viadck on Fri, 10 Jul 2026 11:21:43 GMT
View Forum Message <> Reply to Message

Hello everyone,

The current situation regarding the GhostLock root exploit (CVE-2026-43499) has reached a critical bottleneck for hosting providers running production workloads on OpenVZ 7.

According to official ecosystem roadmaps, OpenVZ 7 is supposed to remain supported. Yet, we are currently facing a severe, host-breaking local privilege escalation vulnerability with no clear path to mitigation or patching for open-source OpenVZ users.

The Corporate & Licensing Trap

Let's look at the reality of the WebPros ecosystem:

1. Virtuozzo maintains OpenVZ.

2. WebPros owns Virtuozzo, as well as SolusVM, which is actively licensed as management software for KVM and OpenVZ VPS nodes.

3. Due to internal corporate partnerships, third-party tools like KernelCare do not support OpenVZ 7, pointing users directly to Virtuozzo's native ReadyKernel instead.

This has created an absolute trap. My production host nodes are fully up to date on disk, running the latest stable release: 3.10.0-1160.119.1.vz7.224.4. However, running readykernel info yields Loaded patches: 0. Why? Because WebPros/Virtuozzo gatekeeps the live patch repository behind licensing channels that SolusVM/OpenVZ customers are not even given an option to purchase or order in their portals.

SolusVM support is currently deflecting tickets by stating that OpenVZ 7 security coverage is uncertain and that it's a "vendor issue." WebPros is the vendor for both sides of this equation. You cannot license orchestration software for a virtualization tier, block third-party security vendors, and then completely abandon the community when a major exploit hits.

If anyone from Virtuozzo or WebPros engineering is monitoring this forum, we need an official kernel update pushed to the public repositories immediately, or the ReadyKernel patch channels opened up for this critical CVE.

Leaving paying ecosystem customers stranded with an active root exploit because of broken licensing workflows is unacceptable.

Kind regards!