Subject: CVE-2026-72389 (Bridge STP UAF) OpenVZ 7 kernel update planned?
Posted by viadck on Thu, 10 Sep 2026 17:13:30 GMT
View Forum Message <> Reply to Message

Hi,

A new Linux kernel vulnerability, CVE-2026-72389, has been disclosed affecting the bridge STP code:

We are still running OpenVZ 7 production nodes and, after the recent GhostLock issue, I wanted to check whether an official OpenVZ 7 kernel update is planned for this CVE.

I have inspected the source of the OpenVZ 7 kernel we are currently running, based on:

3.10.0-1160.119.1.vz7.224.4

and the vulnerable code appears to be present.

In particular, br_topology_change_detection() does not contain the new IFF_UP check, and br_dev_delete() does not synchronously shut down the STP timers before unregistering the bridge device.

We also tested capability reachability inside a normal OpenVZ 7 container. The container has CAP_NET_ADMIN and was able to successfully create a Linux bridge with:

ip link add br-cve-test type bridge

We did not attempt to reproduce the UAF or run an exploit, but this seems sufficient to consider the issue relevant to OpenVZ 7 containers sharing the host kernel.

Could you please confirm:

- Is OpenVZ 7 considered affected by CVE-2026-72389?
- Is an updated vzkernel containing the fix planned?
- If so, will it first be published in the factory repository as happened with the recent GhostLock update?

Current production kernel in our case is based on .vz7.224.4.

Thanks again for your help with the previous GhostLock issue.