Subject: Re: CVE-2026-72389 (Bridge STP UAF) OpenVZ 7 kernel update planned?
Posted by wiredincode on Fri, 11 Sep 2026 12:53:44 GMT
View Forum Message <> Reply to Message

It appears that OpenVZ would be vulnerable to this. I didn't even know about the "Factory" repo, so glad you mentioned this as I made my own patch for Ghostlock.

Note current factory repo version is 3.10.0-1160.129.1.vz7.226.3, not .224.4.

From my initial investigation, it appears you can mitigate this by disabling the Bridge feature on your containers:

[root@chivz23-new ~]# vzctl exec 7570 'ip link add testbr type bridge && echo "EXPOSED" || echo "blocked"'
EXPOSED

[root@chivz23-new ~]# vzctl exec 7570 ip link del testbr

[root@chivz23-new ~]# vzctl set 7570 --features bridge:off --save --setmode restart
Unable to set features for the running Container
Restart the Container
Stopping the Container ...
[...]
Container start in progress...
Saved parameters for Container 7570

[root@chivz23-new ~]# vzctl exec 7570 'ip link add testbr type bridge && echo "EXPOSED" || echo "blocked"'
RTNETLINK answers: Permission denied
blocked

I can't make any guarantees but there is some logic to the fact that if you can't open a bridge, you can't mess with the timers, so I am applying this mitigation to my containers while I test my kernel patch.