Red Hat Patches 9.8-Rated Linux TCP Flaw; Ubuntu Fixes Still in Testing



Fixed kernels for CVE-2026-98432, a remotely reachable use-after-free in the Linux kernel's IPv4 TCP code, are available for RHEL 8, 9 and 10. Ubuntu's fixes remain in an opt-in testing channel.

- CVE-2026-98432 is a use-after-free in the Linux kernel's IPv4 TCP code, rated 9.8.
- A remote, unauthenticated attacker can reach the flaw.
- Fixed kernels are available for Red Hat Enterprise Linux 8, 9 and 10.
- Ubuntu's fixes for its three newest LTS releases are only in an opt-in testing channel.
- No date has been given for a regular Ubuntu update.

Fixed kernels are now available for a critical flaw in the Linux kernel's IPv4 TCP code. The issue, tracked as

CVE-2026-98432, is a use-after-free vulnerability with a severity rating of 9.8.

What is known

The flaw can be reached by a remote, unauthenticated attacker, which is why it carries such a high rating. Red Hat has released fixed kernels for Red Hat Enterprise Linux 8, 9 and 10.

Ubuntu's position is different. Fixes for its three newest long-term-support releases are available only in an opt-in testing channel, and no date has been given for delivery through the regular update path.

Why it matters

The vulnerable code sits in the kernel's network stack, so any Linux host that accepts IPv4 TCP traffic should be reviewed. Because the source article is truncated, details such as exploitation status and exact impact are not covered here, and teams should check the vendor advisories directly.

Recommended approach

Red Hat environments can move to patching through normal change control, prioritising systems reachable from untrusted networks. For Ubuntu, teams must decide whether to use the testing-channel fixes on exposed systems or to apply interim controls until a regular update is released. Kernel updates generally require a reboot, so maintenance windows should be planned in advance.

What to do now

1. Inventory Linux hosts running RHEL 8, 9, 10 and Ubuntu LTS releases, noting which are reachable from the internet or untrusted networks.
2. Schedule Red Hat kernel updates under emergency change control, starting with exposed systems, and plan the required reboots.
3. For Ubuntu, decide through risk acceptance whether to use the testing-channel fixes on exposed hosts or apply interim network restrictions.
4. Monitor Ubuntu advisories for the regular update and patch promptly when it is released.
5. Record the exposure and remediation status for vulnerability-management reporting.