Weekly Threat Roundup: PHP, GitLab, Linux, Node.js and LiteLLM Issues Among Week's Headlines



The Hacker News ThreatsDay roundup lists a busy week: critical PHP and GitLab RCE flaws, Linux bugs, compromised eMudhra certificates, a Node.js RCE, a hacked LiteLLM release and hijacked Tor relays.

- Critical remote code execution flaws were reported in PHP and GitLab.
- Serious Linux security bugs and a Node.js RCE flaw featured this week.
- eMudhra certificates were reported compromised.
- A LiteLLM release was hacked, and hundreds of Tor relays were hijacked.
- The roundup also headlines an AI secrets leak, PingCAP source theft, a Signal flaw and a Laravel authentication bypass.

The Hacker News weekly ThreatsDay roundup describes a demanding few days for security teams, with several significant items reported before the week had even ended.

What was reported

The headline items include critical remote code execution (RCE) flaws in PHP and GitLab, serious Linux security bugs, and an RCE flaw in Node.js. Beyond vulnerabilities, the roundup points to compromised eMudhra certificates, a hacked LiteLLM release, and hundreds of hijacked Tor relays.

The item's title also names an AI secrets leak, source code theft at PingCAP, a Signal flaw involving call hang-up, and a Laravel authentication bypass, along with 21 further stories. The excerpt available to us does not give technical details, affected versions, CVE identifiers or fixes for any of these, so teams should consult the original reporting and vendor advisories before acting.

Why it matters

The mix spans web frameworks, developer platforms, operating systems, certificate infrastructure and AI tooling. These are common components in regulated environments, and the supply chain and secrets-exposure themes are relevant to any institution that uses open-source packages or AI libraries.

Suggested approach

Treat the roundup as a prompt for an inventory check rather than an emergency. Confirm which of the named products you run, read the vendor advisories, and prioritise internet-facing systems and developer pipelines.

What to do now

1. Check your asset inventory for PHP, GitLab, Node.js, Linux, Laravel and LiteLLM and note versions in use.
2. Review vendor advisories and apply available patches, starting with internet-facing systems.
3. Verify the source and integrity of LiteLLM and other AI or open-source packages pulled into builds.
4. Check whether certificates issued by eMudhra are in use and follow the issuer's guidance.
5. Scan repositories and CI pipelines for exposed secrets and rotate any that are found.