Weekly Threat Roundup: PHP, GitLab, Linux, Node.js and LiteLLM Issues in One Week



A threat roundup lists critical PHP and GitLab RCE flaws, Linux bugs, compromised eMudhra certificates, a Node.js RCE, a hacked LiteLLM release and hijacked Tor relays. The source gives only headlines.

- The roundup cites critical remote code execution flaws in PHP and GitLab.
- It also mentions serious Linux security bugs and a Node.js RCE flaw.
- eMudhra certificates are described as compromised, and a LiteLLM release as hacked.
- Hundreds of Tor relays are reported hijacked.
- The item's title also names an AI secrets leak, PingCAP source theft, a Signal flaw and a Laravel authentication bypass; the excerpt gives no detail on them.

A weekly threat roundup from The Hacker News describes a heavy few days for defenders. The excerpt available to us lists headline items only, so this note does not go beyond what it states.

What was reported

The roundup names critical remote code execution flaws in PHP and GitLab, serious Linux security bugs, and a remote code execution flaw in Node.js. It also refers to compromised eMudhra certificates, a hacked LiteLLM release and hundreds of hijacked Tor relays. The full title adds an AI secrets leak, theft of PingCAP source code, a Signal flaw and a Laravel authentication bypass, among other items.

The excerpt gives no CVE numbers, affected versions, patch status or technical detail. Those must be taken from the vendors' own advisories.

Why it matters for your estate

PHP, GitLab, Linux, Node.js and Laravel are common in enterprise and development environments, and a compromised software release or certificate can affect systems that were not otherwise exposed. Organisations should check whether they run any of the named components and confirm the details with the primary sources before acting.

What to do now

1. Check your asset and software inventories for PHP, GitLab, Linux, Node.js, Laravel and LiteLLM.
2. Review the vendors' own advisories for the named flaws and apply patches according to your change process.
3. If LiteLLM is used, confirm which release is deployed and whether it is the affected one.
4. Check whether any certificates issued by eMudhra are in use and follow the issuer's guidance.
5. Review secrets handling in AI and development tooling, and rotate credentials if exposure is suspected.