

Forum:[Hack Forums](#)

Thread: [CVE-2025-12735 expr-eval Remote Code Execution Nightmare](#)

JoseMar - November 10, 2025, 7:20 am

CVE-2025-12735 – expr-eval

Remote Code Execution Nightmare

This vulnerability

When i read about this vulnerability, my first thought was, huh, of course it's the math parser. CVE-2025-12735 hits expr-eval, you know, the little library people use to avoid eval(), the “safe” math evaluator. Turns out not-so-safe, because attackers can inject functions into the parser context and execute system commands. Remote code execution, real-world impact, not the usual hype.

It's worse than a single package though, 250+ dependents,so AI/NLP stacks that process user-supplied expressions are prime targets.

Carnegie Mellon folks flagged the issue, and Jangwoo Choe (UKO) handled the responsible disclosure and the patch are via GitHub PR #288. The patched release is expr-eval-fork v3.0.0, introduces an allowlist, forces custom functions to be registered, and beefs up tests. Also, look up GitHub Security Advisory GHSA-jc85-fpwf-qm7x if you want the advisory.

Why does this rinse-and-repeat feel familiar? Because we copy packages, trust transitive deps, and then shrug when things break. npm audit will flag it, sure, but audits are only useful if someone actually runs them and reads the results instead of ignoring the noise. If your server evaluates user expressions, update now, like actually update, and re-evaluate what you let user input reach.

Anyway, I'm rambling because this is exactly the kind of tiny thing that spirals, you patch one library and five others become suspicious.