

Forum: [Hack Forums](#)

Thread: [n8n hit with CVE-2025-68613, CVSS 9.9, patch ASAP](#)

JoseMar - December 23, 2025, 2:39 am

n8n hit with CVE-2025-68613, CVSS 9.9, patch ASAP

The workflow automation tool n8n a lot of people treat like plumbing, just got hit with a critical vuln. And not the cute kind.

arbitrary code

So apparently there's a vulnerability, CVE-2025-68613, CVSS 9.9. That's basically a red siren. If an authenticated user messes with expressions during workflow config, under certain conditions they can break out and run arbitrary code. Not sandboxed enough. Runtime gets exposed. You know where this goes.

Arbitrary code execution as the n8n process. Full compromise territory. Data access, workflow tampering, system-level stuff. The whole nightmare bundle.

And this thing has like 57k weekly downloads on npm. Not niche. Not obscure.

What really got me though is the number of exposed instances. Over 100k potentially vulnerable as of December 22. Mostly US, Germany, France, Brazil, Singapore. That's... a lot of blast radius. Makes you wonder how many people even know they're running it publicly.

Patch now, think later

So, here are affected versions from 0.211.0 up to before 1.120.4. It is patched now, 1.120.4, 1.121.1, 1.122.0. But let's be real, how many prod setups lag behind?

If you can't patch immediately, at least lock down who can create or edit workflows. Harden the environment. Drop privileges. Limit network access. Basic damage control.

Honestly, this feels like one of those "quiet until it's not" bugs. Curious how many compromises we'll hear about in a few weeks. Or maybe we won't. That's usually worse.