Anthropic VS code extension on Cursor backdoored for nearly 12 hours

An official extension for Anthropic's Claude model was backdoored and threatened as many as 5,000 developers' machines, multiple sources reported Friday. Anthropic so far has yet to warn customers of the incident.

The compromised package was a VS Code extension available in the marketplace of Cursor, a maker of AI-assisted developer tools, the company said Friday. The malicious version, 2.1.313, subsequently affected "at most 5,000 users," presumably when they either downloaded it or their systems automatically fetched and installed it. Anthropic pushed version 2.1.314 several hours after the previous version became available on Cursor, according to independent researcher Kevin Beaumont. Both Beaumont and the CTO and co-founder of security firm Phorian said that version 2.1.313 was distributed through Anthropic's official account on Cursor. So far, neither Cursor nor Anthropic has explained how the attackers gained control of the account.

In search of cloud credentials

"It was a supply-chain compromise where the attacker gained access to the official distribution channel," Phorian CTO and co-founder Luke Roberts told Ars. "The malicious version 2.1.313 was posted to the official Anthropic account, effectively superseding 2.1.312. Extensions auto-update in Cursor by default, but users can configure this in settings." Phorian has more details here.

Read full article

Comments

https://arstechnica.com/security/2026/10/anthropic-vs-code-extension-on-cursor-backdoored-for-nearly-12-hours/