Tampered Claude Code Extension Stayed in Cursor's Marketplace for 11 Hours

Kabui, Charles

2026-11-13

Read at ToKnow.ai



Cursor is an AI code editor that loads extensions, add-ons that run with the developer's own access. On October 29, a tampered copy of Anthropic's Claude Code extension sat in Cursor's own marketplace for about 11 hours, from 2:27 a.m. to 1:35 p.m. Pacific time. It used the real extension's name, and Cursor updates extensions automatically by default. Security firm Phorion found the added code ran as soon as the extension loaded. It tried to add the

attacker's key to the computer's list of keys allowed to log in, like a spare front-door key, and to open a connection out to the attacker's server. Cursor first said at most 5,000 users were affected.

Developer computers often hold source code and cloud accounts. Cursor says turning on remote login needs administrator rights the extension lacks on most Macs and Windows PCs, so the attacker could not log in there. The key, startup scripts and a report of the computer's name and IP address still went through, and uninstalling the extension may not remove them. Security firm Expel saw malicious activity on four customers' Macs, one starting about 8 hours after Cursor pulled the copies. Anthropic says its own systems were not breached. By November 10, neither company had said how the attacker got in. Anyone who installed or updated it that day can search the .ssh folder's authorized_keys file for a key labelled svc-telemetry. Team admins can delay new extension versions by some hours, but the delay is off by default.

Read More: Kickbacks.ai, another VS Code extension that rewrites a Claude Code install on the developer's own machine

Sources:

- Security notice: malicious versions of Anthropic.claude-code in the Cursor VS Code Extension Marketplace (Cursor)
- Anthropic VS code extension on Cursor backdoored for nearly 12 hours (Ars Technica)
- Cursor removes malicious Claude Code extension after SSH backdoor attempt (CSO Online)
- Fake Claude Code extension in Cursor: How to find the backdoor (Expel)
- Extensions (Cursor documentation)

Disclaimer: *For information only. Accuracy or completeness not guaranteed. Illegal use prohibited. Not professional advice or solicitation.* ***Read more:*** */terms-of-service*