CHECKLIST · SCAMS & SECURITY

A tampered Claude Code extension left a back door on Cursor users' computers

Published 31 October 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/cursor-claude-code-extension-backdoor/

- [ ] **Check whether Cursor updated Claude Code overnight on 29–30 October.** If it installed version 2.1.312 or 2.1.313 from Cursor's marketplace on a Mac or Windows PC, run the key check on that computer.
- [ ] **Look for the attacker's SSH key.** On a Mac, search ~/.ssh/authorized_keys for svc-telemetry. On Windows, search %USERPROFILE%\.ssh\authorized_keys and C:\ProgramData\ssh\administrators_authorized_keys. If the key is there, the computer is affected.
- [ ] **Disconnect an affected computer.** Take it off the network before cleaning it, and ask your IT provider whether to rebuild it.
- [ ] **Run Cursor's clean-up script.** Download it from Cursor's Claude Code extension security notice. On a Mac, run it as the affected user, not as root; on Windows, run it in PowerShell as administrator.
- [ ] **Change passwords and keys from a different computer.** Rotate API keys, cloud logins and access tokens that were stored or used on the affected machine, and sign out its sessions.
- [ ] **Give your IT provider Cursor's indicators.** Ask them to search logs for connections to the address 134.209.82.225 and for the file hashes in Cursor's notice.

NOTES

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.