Cursor links trojanized Claude Code extension to access key exposed in Fireworks AI breach



Cursor says the compromise of Anthropic's Claude Code extension on its marketplace came from an access key it issued to Fireworks AI, which was exposed after a breach there. The attacker used it to copy data from a read-only source.

- Cursor says the trojanized Claude Code extension on its marketplace resulted from a stolen access key.
- The key had been issued by Cursor to Fireworks AI.
- Fireworks AI exposed the key after a breach targeting it, according to Cursor.
- The attacker used the key to copy data from a read-only resource.
- The source excerpt is partial and does not give further technical detail.

Cursor has explained how an official Claude Code extension from Anthropic was compromised on its extension marketplace. In an update, the company said an attacker obtained an access key that Cursor had issued to Fireworks AI.

What the source says

According to Cursor, the key was exposed by Fireworks AI following a breach that targeted that company. The attacker then used the key to copy data from a read-only resource. The source excerpt is cut off at this point, so it does not describe what the data was, how it was then used to alter the extension, or how many users were affected.

Why it matters for regulated institutions

The incident shows how a credential held by a third party can become the entry point into a trusted distribution channel. Developer tools and IDE extensions often run with broad access to source code and internal systems, so a tampered extension is a supply-chain concern even when the original weakness sits with a supplier's supplier.

Institutions should avoid drawing conclusions beyond what has been published. Cursor and the other parties may release further details, and teams should track those updates before deciding on wider remediation.

In the meantime, this is a sensible moment to review which AI coding tools and extensions are in use, who issued the credentials they rely on, and how quickly those credentials could be revoked if a partner is breached.

What to do now

1. Inventory the AI coding assistants and IDE extensions in use across engineering teams, including Cursor and Claude Code.
2. Check the vendors' published advisories and follow any remediation steps they issue for the affected extension.
3. Review keys and tokens issued to third-party AI providers, and confirm each is scoped to least privilege and can be revoked quickly.
4. Rotate credentials shared with suppliers whenever a supplier reports a breach.
5. Add extension sources and versions to third-party risk reviews under your NCA ECC and SAMA CSF supply-chain controls.