OpenCode Breach Exposes API Keys Used With External Providers



The open-source AI coding project OpenCode told a small number of users that API keys they used with external providers were exposed in a security breach. Affected teams should rotate those keys.

- OpenCode is an open-source AI coding project.
- It notified a small number of users about a security breach.
- The exposed data were API keys used with external providers.
- The source frames the incident amid AI distillation attacks.
- Only the opening of the report was available, so further details are unconfirmed.

What was reported

OpenCode, an open-source AI coding project, has informed a small number of its users that API keys they had used with external providers were exposed in a security breach. BleepingComputer reports the incident in the context of ongoing AI distillation attacks.

What is not yet known

The portion of the report available to us does not describe how the breach happened, when it occurred, which providers were involved, or whether the keys were misused. We have therefore not included any of those details. Readers should consult the original report and any notice from the project for updates.

Why it matters for regulated institutions

Developers increasingly connect AI coding tools to external model providers using API keys. A key exposed through a third-party tool can be used by others to consume services under the organisation's account, and may reveal what the account is permitted to access. Even where only a small number of users are affected, any team that has used such a tool with provider keys should treat the possibility of exposure seriously.

The practical response is straightforward: find out whether anyone in the organisation uses the tool, rotate any keys that were configured in it, and review provider usage logs for activity that cannot be explained.

What to do now

1. Check whether developers or teams in your organisation use OpenCode.
2. Rotate any provider API keys that were configured in OpenCode, without waiting for confirmation of misuse.
3. Review usage and billing logs at each provider for unexplained activity.
4. Restrict key scope and set spending limits where the provider allows.
5. Move API keys into a managed secrets store and add AI coding tools to your third-party and approved-software inventory.