CHECK

The extension security checklist

Free guide. No signup. 2 min read

Checked 2026-10-31 against Cursor's own notice: cursor.com/blog/claude-code-extension-security-notice (Oct 29, 2026, updated Oct 30 at 11:30 am PT).

From @learningwithcole

On October 29, 2026, malicious copies of the Claude Code extension sat in the Cursor extension marketplace. Cursor says Anthropic did not build them. Here is how to check your machine and what to do with the answer. Everything below comes from Cursor's notice.

Are you in scope?

You only need this if you installed or updated to `Anthropic.claude-code` version 2.1.312 or 2.1.313 from the Cursor VS Code extension marketplace, on Mac or Windows, between 2:27am PT and 1:35pm PT on October 29, 2026.

Cursor says it has no evidence that other versions of the extension or the official distribution are affected.

Run the check

The malicious extension adds an attacker's public key, labeled `svc-telemetry`, to your SSH authorized keys.

Mac: paste this into Terminal.

JavaScript

```
grep -qs svc-telemetry ~/.ssh/authorized_keys && echo "svc-telemetry key found" || echo "No key found; machine not impacted"
```

Windows: paste this into PowerShell.

JavaScript

```
$files = "$HOME\.ssh\authorized_keys",
"C:\ProgramData\ssh\administrators_authorized_keys" | Where-Object { Test-Path $_ }
if ($files -and (Select-String svc-telemetry $files)) { "svc-telemetry key found" }
else { "No key found; machine not impacted" }
```

What the result means

- `No key found; machine not impacted`: that check came back clean.
- `svc-telemetry key found`: your machine is impacted. Keep going.

If the key is found

Don't just uninstall the extension. Cursor says that may not be enough, because the payload drops standalone persistence scripts that keep running.

1. Isolate the machine.
2. Download Cursor's cleanup script for your platform from the notice. It removes the malicious extension, the persistence, the running tunnel processes and the attacker's SSH key. It exits with a non-zero status if anything remains.
   - Mac: save `remediate-macos.sh`, then run this as your normal user, not as root, from the folder you saved it to: `bash remediate-macos.sh`
   - Windows: save `remediate-windows.ps1`, open PowerShell with Run as Administrator, and run this from the folder you saved it to:
     `powershell -ExecutionPolicy Bypass -File .\remediate-windows.ps1`
3. Decide whether the machine should be rebuilt.
4. From a trusted machine, rotate the credentials and sessions that were reachable from the affected one.

What it did, and what it couldn't do

- It collected host details: hostname, username, OS, architecture, home directory path, environment variable names, working directories, Git email and public IP.
- It tried to add the SSH key, turn on the local SSH service and open a reverse SSH tunnel, then keep that tunnel alive with a LaunchAgent on Mac or a scheduled task on Windows.

- Cursor says the attacker's server no longer works, so the reverse shell and the host-detail reporting are not functional.
- Turning on the SSH service needs admin rights, which the extension doesn't have on most Mac and Windows machines. On those machines the attacker could not have logged in through the tunnel.
- Even so, Cursor says the extension added the attacker's key, installed persistence and sent host details.

Cursor's advice is to follow the cleanup steps regardless.

Questions go to security@cursor.com.