

VIRUS DURCH CLAUDE-SKILLS: ALLE SKILLS MIT NVIDIA SKILLSPECTOR SCANNEN

2 PROMPTS

TOOL: CLAUDE CODE

STAND 2026-10-14

Du lässt einmal einen kostenlosen Scanner von NVIDIA über alle Skills laufen, die bei dir in Claude Code installiert sind, und siehst danach schwarz auf weiß, welcher Skill sicher ist und welcher nicht. Alles läuft über einen einzigen Prompt, Claude installiert den Scanner selbst. Dazu kommt der zweite Prompt, mit dem du jeden neuen Skill prüfst, bevor er überhaupt auf deinen Rechner kommt.

1 von 4

SKILLS MIT MINDESTENS EINER SICHERHEITSLÜCKE

1 von 20

SKILLS MIT MUSTERN, DIE STARK NACH ABSICHT AUSSEHEN

17

RISIKOKATEGORIEN, DIE DER SCANNER PRÜFT

0 €

KOSTET DER SCANNER

WAS DU BRAUCHST

Claude Pro oder Max (Pro: 18 € im Monat). Claude Code ist in diesen Abos enthalten.

Claude Code auf deinem Mac oder Windows-PC. Claude Code ist der Claude-Assistent, der direkt auf deinem Rechner arbeitet: Er kann Programme installieren und Dateien lesen. Technisch läuft er im Terminal, du schreibst ihm aber ganz normal wie in einem Chat.

Python 3.12 oder neuer. Python ist eine Programmiersprache, die der Scanner braucht. Fehlt sie, installiert Claude sie im Laufe der Einrichtung für dich, du musst nur zustimmen.

WENN DAS NICHT KLAPPT

Falls dir ein anderer Preis angezeigt wird: Den aktuellen Preis für dein Land siehst du auf claude.com/pricing. Claude Code ist in jedem bezahlten Claude-Abo enthalten.

WARUM SKILLS EIN RISIKO SIND

Ein Skill ist ein Ordner mit einer Datei namens `SKILL.md`: Anweisungen, die Claude befolgt, sobald der Skill passt. Oft liegen daneben kleine Programme, die Claude ausführt. Du liest diese Dateien beim Installieren in der Regel nicht.

Forscher haben 42.447 Skills aus zwei großen Marktplätzen gesammelt und 31.132 davon untersucht. 26,1 % hatten mindestens eine Sicherheitslücke, bei 5,2 % sahen die Muster stark nach Absicht aus. Am häufigsten: Daten, die heimlich nach außen geschickt werden (13,3 %).

Betroffen bist du, wenn du dir mal einen Skill aus dem Internet geholt hast. Skills, die du selbst gebaut hast, sind nicht das Problem.

01 CLAUDE CODE ÖFFNEN

Öffne Claude Code und wähle einen beliebigen Ordner als Arbeitsordner, zum Beispiel einen neuen leeren Ordner auf dem Schreibtisch. Der Scanner selbst wird nicht in diesen Ordner installiert, Claude braucht nur einen Ort, an dem er arbeiten darf.

01 MEINEN PROMPT EINFÜGEN

Kopier den Prompt unten in den Claude Code Chat und schick ihn ab. Claude installiert den Scanner und scannt deine Skills.

Unterwegs fragt Claude mehrmals, ob er einen Befehl ausführen darf. Lies kurz mit und klick auf **Erlauben** bzw. **Yes**. Der Durchlauf dauert meist ein paar Minuten.

`--no-llm` heißt: Der Scanner prüft nur den Text und den Code der Skills und braucht dafür keinen eigenen API-Schlüssel.

SKILLS SCANNEN

```
Installiere NVIDIA SkillSpector (github.com/NVIDIA/SkillSpector). Scanne danach alle Skills in ~/.claude/skills und .claude/skills mit --no-llm. Erklär mir auf Deutsch und einfach, welcher Skill sicher ist und welcher nicht, und warum.
```

WENN DAS NICHT KLAPPT

Alternativer Weg zum selben Ergebnis: Schick Claude zuerst nur „Installiere SkillSpector mit uv tool install git+https://github.com/NVIDIA/skillspector.git“. Wenn das durchgelaufen ist, schick „Scanne mit skillspector scan alle Skills in ~/.claude/skills mit --no-llm und erkläre mir das Ergebnis auf Deutsch“.

DAS ERGEBNIS LESEN

Für jeden Skill bekommst du einen Risiko-Wert von 0 bis 100. Je höher, desto gefährlicher. Dazu ein Urteil und bei jedem Fund die genaue Datei und Zeile.

SAFE (0 bis 20): keine auffälligen Muster gefunden. Du kannst den Skill weiter nutzen.

CAUTION (21 bis 50): Lass dir von Claude erklären, was genau gefunden wurde, und entscheide dann.

DO NOT INSTALL (ab 51): Schreib Claude „Lösch diesen Skill von meinem Rechner“. Hast du dem Skill Passwörter oder Zugangsschlüssel anvertraut, ändere sie.

NEUE SKILLS VORHER PRÜFEN

Ab jetzt läuft jeder neue Skill aus dem Internet erst durch den Scanner. Der Scanner nimmt einen GitHub-Link, eine ZIP-Datei, einen Ordner oder eine einzelne **SKILL.md**. Ersetz im Prompt die eckige Klammer durch deinen Link oder den Pfad zur Datei.

Das gilt auch für Skills, die du in der Claude-App hochladen willst: Scann zuerst die ZIP-Datei in Claude Code, lad sie erst danach hoch.

NEUEN SKILL VOR DEM INSTALLIEREN SCANNEN

```
Bevor ich diesen Skill installiere: Scanne ihn mit SkillSpector (--no-llm) und sag mir auf Deutsch, ob ich ihn installieren kann. Hier ist der Skill: [Link zum GitHub-Repo oder Pfad zur ZIP-Datei]
```

DER EHRLICHE TEIL

Ein SAFE ist keine Garantie. Der Scanner liest Text und Code, er führt nichts aus. Was erst beim Ausführen passiert, sieht er nicht. Laut NVIDIA übersieht er außerdem leichter Muster in anderen Sprachen als Englisch. Ein deutscher Skill wird also nicht so gründlich geprüft wie ein englischer.

Die meisten Skills sind harmlos. Der Scan ersetzt nicht den gesunden Menschenverstand: Skills von bekannten Quellen sind sicherer als eine Datei von einem Account, den du nicht kennst.

WENN DAS NICHT KLAPPT

Claude meldet, dass Python fehlt oder zu alt ist: Schreib „Installier mir Python 3.12 und versuch es dann nochmal“.

Die Installation bricht ab: Schreib „Installier SkillSpector mit uv tool install git+https://github.com/NVIDIA/skillspector.git“. Das ist der kurze Weg, den NVIDIA selbst angibt.

Claude findet keine Skills: Dann liegen deine Skills woanders. Frag Claude „Wo sind bei mir Skills installiert?“ und lass genau diese Ordner scannen.

Claude Code reagiert nicht mehr: Schließ Claude Code, öffne es neu und schick den Prompt noch einmal.

HINWEIS

Hinweis: Dieser Guide dient zu Informations- und Bildungszwecken. Alle Inhalte spiegeln den Stand bei Erstellung wider. Oberflächen, Funktionen und Preise der genannten Tools können sich ändern. Prüfe Ergebnisse von KI-Tools immer selbst nach. @GPTMarlon übernimmt keine Haftung für Entscheidungen auf Grundlage dieser Inhalte.