CVE-2026-22561 - DLL Search Order Hijacking in Claude for Windows installer

Summary

None

DLL Search Order Hijacking in Installer Allows Local Privilege Escalation

Severity

Medium

Base Score: 6.6

CVSS - CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H

Description

None

The Claude for Windows installer (Claude Setup.exe) loaded certain DLLs, including profapi.dll, from its own directory before standard system paths after requesting UAC elevation. An attacker who could place a malicious DLL in the same directory as the installer — for example by distributing the installer bundled inside an archive — could achieve arbitrary code execution with Administrator privileges when a victim ran the installer and approved the UAC prompt. Exploitation required the victim to execute the installer from a directory containing the attacker-controlled DLL.

This issue was fixed in installer version 1.1.3363, release on February 17, 2026. A fixed installer is available from claude.ai/download. Existing Claude Desktop installations are not affected; this issue is limited to the installer executable itself.

Thank you to Kazuma Matsumoto, a security researcher at GMO Cybersecurity by IERAE, Inc., for reporting this `issue.`

CWE ID

None

CWE-427 Uncontrolled Search Path Element

Fixed Version

All versions of the Claude Desktop Windows installer, prior to version 1.1.3363. Installers obtained from claude.ai/download on or after February 17, 2026 contain the fix.

Credits

Kazuma Matsumoto, a security researcher at GMO Cybersecurity by IERAE, Inc