Insecure System-Wide Configuration Loading Enables Local Privilege Escalation on Windows

Moderate **OctavianGuzu** published **GHSA-5cwg-9f6j-9jvx** 11 hours ago

Package

@anthropic-ai/claude-code (npm)

Affected versions	Patched versions
< 2.1.75	2.1.75

Description

On Windows, Claude Code loaded system-wide default configuration from `C:\ProgramData\ClaudeCode\managed-settings.json` without validating directory ownership or access permissions. Because the `ProgramData` directory is writable by non-administrative users by default and the `ClaudeCode` subdirectory was not pre-created or access-restricted, a low-privileged local user could create this directory and place a malicious configuration file that would be automatically loaded for any user launching Claude Code on the same machine. Exploiting this would have required a shared multi-user Windows system and a victim user to launch Claude Code after the malicious configuration was placed.

Users on standard Claude Code auto-update have received this fix already. Users performing manual updates are advised to update to the latest version.

Thank you to hackerone.com/edbr for reporting this issue.

Severity

Moderate 5.4 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Local
Attack Complexity	Low
Attack Requirements	Present
Privileges Required	Low
User interaction	Passive
Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-35603

Weaknesses

▶ CWE-426