INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 17:20 UTC

CVE-2026-35603: Privilege Escalation via Insecure ProgramData in AI Coding Tools

CVE VULNERABILITY | HIGH | CVSS 7.8

SCC Item ID	SCC-CVE-2026-0328
Type	CVE Vulnerability
CVE ID	CVE-2026-35603
Severity	HIGH
CVSS Base Score	7.8
EPSS Score	0.0011 (1th percentile)
Affected Products	Claude Code (Anthropic), Cursor, Codex CLI (OpenAI), Gemini CLI (Google), Windows platform; specific patched versions unconfirmed from verified sources
Published	2026-06-17
Discovery Source	Gemini

Executive Summary

CVE-2026-35603 is a high-severity privilege escalation vulnerability affecting AI-assisted coding tools on Windows, including Claude Code (Anthropic), Cursor, Codex CLI (OpenAI), and Gemini CLI (Google). A low-privileged local attacker can exploit insecure ProgramData directory permissions to execute arbitrary commands under an administrator's security context. Organizations with developers running these tools on Windows workstations face elevated risk of local privilege escalation leading to credential theft, lateral movement, or workstation compromise.

Technical Analysis

CVE-2026-35603 (CVSS 7.8 High) describes a local privilege escalation condition rooted in insecure Windows ProgramData directory configurations across multiple AI coding tool installations. The root weaknesses are CWE-427 (Uncontrolled Search Path Element), CWE-732 (Incorrect Permission Assignment for Critical Resource), and CWE-269 (Improper Privilege Management). Affected products: Claude Code (Anthropic), Cursor, Codex CLI (OpenAI), and Gemini CLI (Google) on Windows; specific patched version numbers are not confirmed from verified upstream sources at this time. Attack vectors map to MITRE ATT&CK T1574.009 (Path Interception by Unquoted Path), T1574.010 (Services File Permissions Weakness), and T1068 (Exploitation for Privilege Escalation). Exploitation requires local access and targets ProgramData directories with world-writable or inadequately ACL-restricted permissions, enabling DLL planting, binary replacement, or script injection

executed by a privileged process. Anthropic has issued a patch for Claude Code. Cursor, OpenAI, and Google have not confirmed remediation as of the discovery date; Cursor and the CLI vendors are reported to have triaged at low severity or have not responded conclusively. CVSS vector pending NVD publication. EPSS score is 0.00108 (1.4th percentile), indicating low current exploitation probability. Not listed in CISA KEV. Vendor CVSS scores not yet published as of this advisory date. NVD entry exists; source verification was performed upstream prior to publication.

Action Checklist

1. Step 1: Containment. Inventory all Windows developer workstations running Claude Code, Cursor, Codex CLI, or Gemini CLI. Restrict local user accounts on affected machines to the minimum required privileges using NIST AC-6 (Least Privilege) and CIS Benchmarks for Windows (e.g., CIS Microsoft Windows Server 2022 Benchmark v1.x, Section 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts). Prevent developer tool processes from running under elevated accounts until patched versions are confirmed deployed.
2. Step 2: Detection. Audit ProgramData directory ACLs on Windows developer workstations for world-writable permissions using icacls or equivalent tooling. Review Windows Security Event Log for Event ID 4688 (process creation) showing unexpected child processes spawned from AI coding tool executables, and Event ID 4672 (special privileges assigned) for abnormal privilege grants. Monitor for DLL load events from ProgramData subdirectories associated with Claude Code, Cursor, Codex CLI, or Gemini CLI using Sysmon Event ID 7 (ImageLoaded) filtered to those paths. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS Controls v8 8.2 (Collect Audit Logs) or equivalent Windows audit policy configuration.
3. Step 3: Eradication. Apply Anthropic's released patch for Claude Code immediately; confirm installation against the vendor advisory at the Anthropic official documentation source. For Cursor, Codex CLI, and Gemini CLI: manually correct ProgramData directory ACLs to remove world-writable permissions and restrict to the installing user and SYSTEM accounts only, pending vendor patches. Use icacls to reset inheritance and apply explicit deny rules for low-privileged users on affected directories. Reference CIS Benchmarks for Windows (CIS 4.6: Securely Manage Enterprise Assets and Software) and NIST CM controls for configuration change management.
4. Step 4: Recovery. Re-audit ProgramData directory ACLs post-remediation to confirm permissions are correctly restricted. Validate that developer tooling continues to function under least-privilege accounts. Monitor Event ID 4688 and Sysmon Event ID 7 for a minimum of 72 hours post-patch to detect any residual exploitation attempts. Confirm no unauthorized executables or DLLs were planted in affected directories prior to patching by performing file integrity monitoring (FIM) or System File Analysis (SFA).
5. Step 5: Post-Incident. Review the organization's software approval and configuration baseline process for AI-assisted developer tools, which are a growing and often insufficiently governed asset class. Implement NIST AC-6 (Least Privilege) and CIS Controls v8 7.1 (Establish and Maintain a Vulnerability Management Process) to ensure third-party developer tools are included in patch management scope. Evaluate whether developer workstations require separation from production network segments given the local-access prerequisite for this class of vulnerability (NIST AC-5: Separation of Duties). Document this event as a case study for AI toolchain supply chain risk in the next GRC review cycle.

Detection Guidance

Focus detection on Windows developer workstations running any of the four affected AI coding tools. Key detection signals: (1) Sysmon Event ID 7 (ImageLoaded), alert on DLL loads from C:\ProgramData subdirectories associated with Claude Code, Cursor, Codex CLI, or Gemini CLI by processes other than those tools' own executables; (2) Windows Security Event ID 4688, flag unexpected child processes spawned from AI coding tool parent processes, especially cmd.exe, powershell.exe, or mshta.exe; (3) Windows Security Event ID 4672, alert on special privilege assignments (SeDebugPrivilege, SeTakeOwnershipPrivilege) granted to sessions originating from low-privileged developer accounts; (4) icacls output auditing, script weekly ACL checks on C:\ProgramData\[tool-specific directories] for (M) or (F) permissions granted to Users or Authenticated Users groups; (5) File integrity monitoring (FIM) or System File Analysis (SFA) on ProgramData subdirectories for unexpected binary or DLL drops. No public IOCs (hashes, IPs, domains) are associated with active exploitation of this CVE at this time. EPSS is 0.00108, indicating exploitation is not currently observed in the wild. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) cadence to these log sources. CIS Controls v8 8.2 (Collect Audit Logs) should be verified as active for endpoint logging on developer workstations.

Framework Mappings

MITRE-ATTACK

- **T1574.009** — Path Interception by Unquoted Path
- **T1068** — Exploitation for Privilege Escalation
- **T1574.010** — Services File Permissions Weakness

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **3.3** — Configure Data Access Control Lists
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1574.009	Path Interception by Unquoted Path	Persistence
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1574.010	Services File Permissions Weakness	Persistence

Sources

Source	URL	Tier
CVE-2026-35603 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-35603	T1
CVE-2026-35603: Claude Code Privilege Escalation Flaw	https://www.sentinelone.com/vulnerability-database/cve-2026-35603/	T3
CVE-2026-35603: AI Coding Tools Privilege Escalation - Cymulate	https://cymulate.com/blog/cve-2026-35603-ai-coding-tools-privilege-...	T3
Google Security Advisory	https://chromereleases.googleblog.com/	T1

Generated 2026-06-18 17:20 UTC by TJS Security Command Center