TCC Database Manipulation via Launchctl and Unprotected SIP, Detection Strategy DET0534

Archived: 2026-04-05 18:15:38 UTC

AN1474

Unauthorized modification of TCC.db followed by elevated process execution under a trusted parent (e.g., Finder, SystemUIServer) or via launchctl environment override. Also includes identification of SIP being disabled, which is highly uncommon and a prerequisite for this abuse path.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	Execution of binaries with TCC protected access under unexpected parent processes such as Finder.app, SystemUIServer, or nsurlsessiond
File Modification (DC0061)	macos:unifiedlog	Modification or replacement of /Library/Application Support/com.apple.TCC/TCC.db or ~/Library/Application Support/com.apple.TCC/TCC.db
Command Execution (DC0064)	macos:unifiedlog	Execution of launchctl with setenv or bootout targeting TCC.db or AppleScript under Finder context
Host Status (DC0018)	macos:unifiedlog	System Integrity Protection (SIP) state reported as disabled

Mutable Elements

Field	Description
ParentProcessName	May vary across macOS versions and user contexts; defenders can tune for known benign cases.
TCCModificationPath	Custom user paths or redirected SQLite DBs may require alternate matching logic.
TimeWindow	Temporal proximity between launchctl setenv and subsequent privileged access can be tuned.
SIPStateCheckInterval	Frequency of SIP integrity checks may vary based on system hardening policies.

Source: https://attack.mitre.org/detectionstrategies/DET0534