

Detection Strategy for System Services: Launchctl, Detection Strategy DET0265

Archived: 2026-04-02 10:48:02 UTC

Analytics

- [macOS](#)

AN0736

Abuse of launchctl to execute or manage Launch Agents and Daemons. Defender perspective: correlation of suspicious plist file creation or modification in LaunchAgents/LaunchDaemons directories with subsequent execution of the launchctl command. Abnormal executable paths (e.g., /tmp, /Shared) or launchctl activity followed by network connections are highly suspicious.

Log Sources

Mutable Elements

Field	Description
MonitoredPaths	Paths to monitor for suspicious plist files, such as /Library/LaunchAgents, /Library/LaunchDaemons, ~/Library/LaunchAgents.
SuspiciousExecPaths	Uncommon executable paths (e.g., /tmp, /Shared) that should raise alerts when associated with launchctl services.
TimeWindow	Correlation window for detecting plist file creation and subsequent launchctl execution.

Source: <https://attack.mitre.org/detectionstrategies/DET0265#AN0736>