Detection Strategy for Exploitation for Privilege Escalation, Detection Strategy DET0514

Archived: 2026-04-02 10:36:15 UTC

AN1419

Detects exploitation attempts targeting vulnerable kernel drivers or OS components, often followed by unusual process or token behavior.

Log Sources

Mutable Elements

Field	Description
DriverNamePattern	Targeted BYOVD drivers may vary based on campaign and tooling.
TimeWindow	Controls temporal linking of driver load → process spawn → privilege use.
ParentProcessPath	Parent-child relationships vary by exploitation vector (e.g., LOLBin vs. dropper).

AN1420

Detects escalation via vulnerable setuid binaries or kernel modules, often chained with unusual access to /proc/kallsyms or /dev/kmem.

Log Sources

Mutable Elements

Field	Description
SetUIDBinaryList	Legitimate SUID binaries vary across distributions; false positives may arise.
TimeWindow	Allows chaining kernel module load with privilege spike or privilege-sensitive process activity.
EffectiveUIDThreshold	Default is uid=0, but environments may vary with containerized root-like accounts.

AN1421

Detects use of vulnerable kernel extensions or entitlements abused via setuid or AppleScript injection chains.

Log Sources

Mutable Elements

Field	Description
EntitlementList	Entitlements vary by app and OS version; some allow unexpected behavior.
TimeWindow	Correlate SUID execution or AppleScript injection with privilege gain or module load.

AN1422

Detects container breakout behavior via exploitation (e.g., DirtyPipe, CVE-2022-0847), followed by host OS interaction or escalated capability assignment.

Log Sources

Mutable Elements

Field	Description
NamespaceEscapePattern	May vary with CVE technique or custom syscall wrapper.
TimeWindow	Controls correlation of breakout → host interaction.
