Privileged Process Integrity, Mitigation M1025 - Enterprise

Archived: 2026-04-05 14:27:54 UTC

Privileged Process Integrity focuses on defending highly privileged processes (e.g., system services, antivirus, or authentication processes) from tampering, injection, or compromise by adversaries. These processes often interact with critical components, making them prime targets for techniques like code injection, privilege escalation, and process manipulation. This mitigation can be implemented through the following measures:

Protected Process Mechanisms:

- Enable RunAsPPL on Windows systems to protect LSASS and other critical processes.
- Use registry modifications to enforce protected process settings: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL`

Anti-Injection and Memory Protection:

- Enable Control Flow Guard (CFG), DEP, and ASLR to protect against process memory tampering.
- Deploy endpoint protection tools that actively block process injection attempts.

Code Signing Validation:

- Implement policies for Windows Defender Application Control (WDAC) or AppLocker to enforce execution of signed binaries.
- Ensure critical processes are signed with valid certificates.

Access Controls:

- Use DACLs and MIC to limit which users and processes can interact with privileged processes.
- Disable unnecessary debugging capabilities for high-privileged processes.

Kernel-Level Protections:

- Ensure Kernel Patch Protection (PatchGuard) is enabled on Windows systems.
- Leverage SELinux or AppArmor on Linux to enforce kernel-level security policies.

Tools for Implementation

Protected Process Light (PPL):

- RunAsPPL (Windows)
- Windows Defender Credential Guard

Code Integrity and Signing:

- Windows Defender Application Control (WDAC)

- AppLocker
- SELinux/AppArmor (Linux)

Memory Protection:

- Control Flow Guard (CFG), Data Execution Prevention (DEP), ASLR

Process Isolation/Sandboxing:

- Firejail (Linux Sandbox)
- Windows Sandbox
- QEMU/KVM-based isolation

Kernel Protection:

- PatchGuard (Windows Kernel Patch Protection)
- SELinux (Mandatory Access Control for Linux)
- AppArmor
