User Account Control, Mitigation M1052 - Enterprise

Archived: 2026-04-05 18:19:33 UTC

User Account Control (UAC) is a security feature in Microsoft Windows that prevents unauthorized changes to the operating system. UAC prompts users to confirm or provide administrator credentials when an action requires elevated privileges. Proper configuration of UAC reduces the risk of privilege escalation attacks. This mitigation can be implemented through the following measures:

Enable UAC Globally:

- Ensure UAC is enabled through Group Policy by setting `User Account Control: Run all administrators in Admin Approval Mode` to `Enabled`.

Require Credential Prompt:

- Use Group Policy to configure UAC to prompt for administrative credentials instead of just confirmation (`User Account Control: Behavior of the elevation prompt`).

Restrict Built-in Administrator Account:

Set `Admin Approval Mode` for the built-in Administrator account to `Enabled` in Group Policy.

Secure the UAC Prompt:

- Configure UAC prompts to display on the secure desktop (`User Account Control: Switch to the secure desktop when prompting for elevation`).

Prevent UAC Bypass:

- Block untrusted applications from triggering UAC prompts by configuring `User Account Control: Only elevate executables that are signed and validated`.
- Use EDR tools to detect and block known UAC bypass techniques.

Monitor UAC-Related Events:

- Use Windows Event Viewer to monitor for event ID 4688 (process creation) and look for suspicious processes attempting to invoke UAC elevation.

Tools for Implementation

Built-in Windows Tools:

- Group Policy Editor: Configure UAC settings centrally for enterprise environments.
- Registry Editor: Modify UAC-related settings directly, such as `EnableLUA` and `ConsentPromptBehaviorAdmin`.

Endpoint Security Solutions:

- Microsoft Defender for Endpoint: Detects and blocks UAC bypass techniques.
- Sysmon: Logs process creations and monitors UAC elevation attempts for suspicious activity.

Third-Party Security Tools:

- Process Monitor (Sysinternals): Tracks real-time processes interacting with UAC.
- EventSentry: Monitors Windows Event Logs for UAC-related alerts.
