Service registry permissions weakness. Let's hunt it!

Search for usage of reg or Powershell by non-privileged users to modify service configuration in registry:

*event_id:1 AND event_data.IntegrityLevel:Medium AND ((event_data.CommandLine:*reg* AND event_data.CommandLine:*add*) OR (event_data.CommandLine:*powershell* AND event_data.CommandLine:("*set-itemproperty*" "* sp *" "*new-itemproperty*"))) AND event_data.CommandLine:(*ControlSet* AND *Services*) AND event_data.CommandLine:(*ImagePath* *FailureCommand* *ServiceDll*)*

task	event_data.ParentImage	event_data.CommandLine	event_data.User	event_data.IntegrityLevel
Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	reg add HKLM\SYSTEM\CurrentControlSet\Services\softinventsvc /v ImagePath /d "C:\temp\winlogon.exe"	WIN10X64_1803\privuser	Medium
Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	reg add HKLM\SYSTEM\CurrentControlSet\Services\softinventsvc /v ImagePath /d "net localgroup Administrators privuser /add"	WIN10X64_1803\privuser	Medium

Medium IL shows us that user is non-privileged