What is a UAC bypass?

A UAC bypass is a Windows technique that elevates an administrator's process from medium to high integrity without showing the User Account Control prompt. UAC normally makes even admin users run at reduced privilege and consent before elevating. Bypasses abuse auto-elevating system binaries (like `fodhelper.exe` or `eventvwr.exe`) that elevate silently, hijacking what they run via the registry. It is technically a same-user integrity jump rather than a cross-user escalation, but it is a common step after gaining an admin foothold.

HOW IT WORKS

01 The abuse and payload

The classic bypass hijacks an auto-elevating binary through the registry:

- The fodhelper technique: create the registry key the binary reads and point it at a command:
- `reg add HKCU\Software\Classes\ms-settings\Shell\Open\command /ve /d "cmd.exe" /f`
- `reg add HKCU\Software\Classes\ms-settings\Shell\Open\command /v DelegateExecute /f`
- run `fodhelper.exe`, which auto-elevates and runs the hijacked `cmd.exe` at high integrity.
- Similar techniques use `eventvwr.exe-`, `computerdefaults.exe`, and others.

Documented techniques shown for defenders.

> NOT A SECURITY BOUNDARY
>
> *Microsoft treats UAC as a convenience barrier, not a hard boundary, so bypasses are common. The real protection is not running as administrator in the first place.*

HOW TO DEFEND

- Set UAC to the highest level ("Always notify") to reduce silent auto-elevation.
- Have users run as standard accounts, not administrators, so a bypass has nothing to elevate.
- Patch promptly, since Microsoft fixes specific auto-elevation paths over time.
- Apply application control to block the hijacked commands.
- Monitor for registry changes under the keys these bypasses abuse (for example `ms-settings\Shell\Open\command`).

SOURCES

[1] Microsoft: How User Account Control works

[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-a-uac-bypass

Open online