What is an unquoted service path?

An unquoted service path is a Windows misconfiguration where a service's executable path contains spaces but is not wrapped in quotes. Windows then tries to run several interpretations of the path in order (treating each space as a possible break), and if an attacker can write an executable at one of those earlier locations, the service runs their program instead, usually as SYSTEM. It is a long-standing, easy-to-find escalation that depends on a writable directory along the path.

HOW IT WORKS

01 The abuse and payload

The attacker finds an unquoted path with a writable segment, plants an executable, and restarts the service:

- Find unquoted paths: `wmic service get name,pathname,startmode | findstr /i /v "C:\Windows\\" | findstr /i /v """`
- Check a writable directory along the path (for example `C:\Program Files\My App\` or `C:\`).
- Place a malicious executable named to match the early break, for example `C:\Program Files\My.exe`.
- Restart the service (or wait for a reboot): `sc stop <svc> & sc start <svc>`. Windows runs the planted binary as the service account, often SYSTEM.

Documented technique shown for defenders.

> TWO CONDITIONS
>
> *An unquoted path is only exploitable when there is also a writable directory along it. Quote the path, or remove the write access, and the escalation disappears.*

HOW TO DEFEND

- Quote every service image path that contains spaces (the simplest fix).
- Audit services for unquoted paths with the wmic query above and correct them.
- Remove write access from directories along service paths, especially `C:\` and `C:\Program Files` subfolders.
- Run services with least privilege so a hijack yields less.
- Monitor for new executables appearing in program directories.

SOURCES

[1] Microsoft: Service Security and Access Rights

[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-an-unquoted-service-path

Open online