What is weak service permissions?

Weak service permissions are a Windows misconfiguration where a low-privileged user can modify a service they should not, by changing its binary path (SERVICE_CHANGE_CONFIG), by replacing the service executable (a writable binary), or by controlling its registry key. Because most services run as SYSTEM, the attacker repoints the service at their own command and restarts it to get SYSTEM. It is found by checking service ACLs and binary permissions with tools like `accesschk`.

HOW IT WORKS

01 The abuse and payload

The attacker enumerates service permissions, then repoints or replaces the service:

- Check permissions: `accesschk.exe -uwcqv <user> *` (services the user can modify) or `sc qc <svc>`.
- Reconfigure the binary path if allowed: `sc config <svc> binPath= "cmd /c net localgroup administrators hacker /add"` then `sc stop <svc> & sc start <svc>`.
- Replace a writable service executable with a malicious one and restart the service.

The action runs as the service account, usually SYSTEM. Documented techniques shown for defenders.

> CHECK ACCESSCHK
>
> *Use* `accesschk.exe -uwcqv "<your-user>" *` *to list services your account can modify. Any service you can reconfigure that runs as SYSTEM is a direct escalation.*

HOW TO DEFEND

- Restrict service permissions so non-admin users cannot change configuration (no SERVICE_CHANGE_CONFIG for standard users).
- Protect service executables so only admins can write them.
- Lock down service registry keys against non-admin writes.
- Run services with least privilege rather than SYSTEM where possible.
- Audit with accesschk-style tooling and monitor for service-config changes.

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-weak-service-permissions

Open online