# TTP Detail – T1058

## TTP Information

Name: Service Registry Permissions Weakness

Description: Windows stores local service configuration information in the Registry under <code>HKLM\SYSTEM\CurrentControlSet\Services</code>. The information stored under a service's Registry keys can be manipulated to modify a service's execution parameters through tools such as the service controller, sc.exe, [PowerShell](https://attack.mitre.org/techniques/T1086), or [Reg](https://attack.mitre.org/software/S0075). Access to Registry keys is controlled through Access Control Lists and permissions. (Citation: MSDN Registry Key Security)

If the permissions for users and groups are not properly set and allow access to the Registry keys for a service, then adversaries can change the service binPath/ImagePath to point to a different executable under their control. When the service starts or is restarted, then the adversary-controlled program will execute, allowing the adversary to gain persistence and/or privilege escalation to the account context the service is set to execute under (local/domain account, SYSTEM, LocalService, or NetworkService).

Adversaries may also alter Registry keys associated with service failure parameters (such as <code>FailureCommand</code>) that may be executed in an elevated context anytime the service fails or is intentionally corrupted.(Citation: TrustedSignal Service Failure)(Citation: Twitter Service Recovery Nov 2017)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation