CAPEC-478: Modification of Windows Service Configuration (Version 3.9)

Archived: 2026-04-05 22:57:23 UTC

Attack Pattern ID: 478 **Abstraction: Detailed**		

Description

An adversary exploits a weakness in access control to modify the execution parameters of a Windows service. The goal of this attack is to execute a malicious binary in place of an existing service.

Likelihood Of Attack

Low

Typical Severity

High

Relationships

This table shows the other attack patterns and high level categories that are related to this attack pattern. These relationships are defined as ChildOf and ParentOf, and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as CanFollow, PeerOf, and CanAlsoBe are defined to show similar attack patterns that the user may want to explore.

Nature	Type
ChildOf	S Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attack. It

This table shows the views that this attack pattern belongs to and top level categories within that view.

View Name	Top Level Categories
Domains of Attack	Software
Mechanisms of Attack	Manipulate System Resources

Execution Flow

Explore

1. **Determine target system:** The adversary must first determine the system they wish to modify the registry of. This needs to be a windows machine as this attack only works on the windows registry.

Experiment

1. **Gain access to the system:** The adversary needs to gain access to the system in some way so that they can modify the windows registry.

Techniques
Gain physical access to a system either through shoulder surfing a password or accessing a system that is left unlocked.
Gain remote access to a system through a variety of means.

Exploit

1. **Modify windows registry:** The adversary will modify the windows registry by changing the configuration settings for a service. Specifically, the adversary will change the path settings to define a path to a malicious binary to be executed.

Prerequisites

The adversary must have the capability to write to the Windows Registry on the targeted system.

Resources Required

None: No specialized resources are required to execute this type of attack.

Consequences

This table specifies different individual consequences associated with the attack pattern. The Scope identifies the security property that is violated, while the Impact describes the negative technical impact that arises if an adversary succeeds in their attack. The Likelihood provides information about how likely the specific consequence is expected to be seen relative to the other consequences in the list. For example, there may be high likelihood that a pattern will be used to achieve a certain impact, but a low likelihood that it will be exploited to achieve a different impact.

Scope	Impact	Likelihood
Integrity	Execute Unauthorized Commands	

Mitigations

Ensure proper permissions are set for Registry hives to prevent users from modifying keys for system components that may lead to privilege escalation.

Taxonomy Mappings

CAPEC mappings to ATT&CK techniques leverage an inheritance model to streamline and minimize direct CAPEC/ATT&CK mappings. Inheritance of a mapping is indicated by text stating that the parent CAPEC has relevant ATT&CK mappings. Note that the ATT&CK Enterprise Framework does not use an inheritance model as part of the mapping to CAPEC.

Relevant to the ATT&CK taxonomy mapping (also see parent)

Entry ID	Entry Name
1574.011	Hijack Execution Flow:Service Registry Permissions Weakness
1543.003	Create or Modify System Process:Windows Service

Content History

Submissions		
Submission Date	**Submitter**	**Organization**
2018-04-25 (Version 2.11)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**
2019-04-04 (Version 3.1)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Weaknesses	
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	
2021-10-21 (Version 3.6)	CAPEC Content Team	The MITRE Corporation
	Updated Description, Execution_Flow	

More information is available — Please select a different filter.
