CAPEC-578: Disable Security Software (Version 3.9)

Archived: 2026-04-06 01:57:53 UTC

Attack Pattern ID: 578 **Abstraction: Standard**		

Description

An adversary exploits a weakness in access control to disable security tools so that detection does not occur. This can take the form of killing processes, deleting registry keys so that tools do not start at run time, deleting log files, or other methods.

Likelihood Of Attack

Medium

Typical Severity

Medium

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	Meta Attack Pattern - A meta level attack pattern in CAPEC is a decidedly abstract characterization of a specific methodology or techniqu

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

Prerequisites

The adversary must have the capability to interact with the configuration of 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
Availability	Hide Activities	

Mitigations

Ensure proper permissions are in place to prevent adversaries from altering the execution status of security tools.

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

Entry ID	Entry Name
1556.006	Modify Authentication Process: Multi-Factor Authentication
1562.001	Impair Defenses: Disable or Modify Tools
1562.002	Impair Defenses: Disable Windows Event Logging
1562.004	Impair Defenses: Disable or Modify System Firewall
1562.007	Impair Defenses: Disable or Modify Cloud Firewall
1562.008	Impair Defenses: Disable Cloud Logs
1562.009	Impair Defenses: Safe Mode Boot

Content History

Submissions		
Submission Date	**Submitter**	**Organization**
2015-11-09 (Version 2.7)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**
2018-07-31 (Version 2.12)	CAPEC Content Team	The MITRE Corporation
	Updated Attack_Motivation-Consequences, Attack_Prerequisites, Description Summary, References, Related_Weaknesses, Resources_Required, Solutions_and_Mitigations, Typical_Likelihood_of_Exploit, Typical_Severity	
2019-04-04 (Version 3.1)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Weaknesses	
2019-09-30 (Version 3.2)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Attack_Patterns	
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Attack_Patterns, Taxonomy_Mappings	
2022-09-29 (Version 3.8)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	
2023-01-24 (Version 3.9)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	

More information is available — Please select a different filter.