CAPEC-558: Replace Trusted Executable (Version 3.9)

Archived: 2026-04-06 00:12:53 UTC

Attack Pattern ID: 558 **Abstraction: Detailed**		

Description

An adversary exploits weaknesses in privilege management or access control to replace a trusted executable with a malicious version and enable the execution of malware when that trusted executable is called.

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	Inject Unexpected Items

Example Instances

Specific versions of Windows contain accessibility features that may be launched with a key combination before a user has logged in (for example when they are on the Windows Logon screen). On Windows XP and Windows Server 2003/R2, the program (e.g. "C:\Windows\System32\utilman.exe") may be replaced with cmd.exe (or another program that provides backdoor access). Then pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over RDP will cause the replaced file to be executed with SYSTEM privileges.

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
1505.005	Server Software Component: Terminal Services DLL
1546.008	Event Triggered Execution: Accessibility Features

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 Description Summary, References, Typical_Likelihood_of_Exploit, Typical_Severity	
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	
2022-09-29 (Version 3.8)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	

More information is available — Please select a different filter.
