CAPEC-17: Using Malicious Files (Version 3.9)

Archived: 2026-04-06 00:28:20 UTC

Attack Pattern ID: 17 **Abstraction: Standard**		

Description

An attack of this type exploits a system's configuration that allows an adversary to either directly access an executable file, for example through shell access; or in a possible worst case allows an adversary to upload a file and then execute it. Web servers, ftp servers, and message oriented middleware systems which have many integration points are particularly vulnerable, because both the programmers and the administrators must be in synch regarding the interfaces and the correct privileges for each interface.

Likelihood Of Attack

High

Typical Severity

Very 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	M Meta Attack Pattern - A meta level attack pattern in CAPEC is a decidedly abstract characterization of a specific methodology or techn
ParentOf	D Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific techni
ParentOf	D Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific techni
ParentOf	D Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific techni
ParentOf	D Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific techni
ParentOf	D Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific techni
ParentOf	D Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific techni
CanFollow	S Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attac

CanFollow	Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attac
CanPrecede	Meta Attack Pattern - A meta level attack pattern in CAPEC is a decidedly abstract characterization of a specific methodology or techn

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	Subvert Access Control

Execution Flow

Explore

1. **Determine File/Directory Configuration:** The adversary looks for misconfigured files or directories on a system that might give executable access to an overly broad group of users.

Techniques
Through shell access to a system, use the command "ls -l" to view permissions for files and directories.

Experiment

1. **Upload Malicious Files:** If the adversary discovers a directory that has executable permissions, they will attempt to upload a malicious file to execute.

Techniques
Upload a malicious file through a misconfigured FTP server.

Exploit

1. **Execute Malicious File:** The adversary either executes the uploaded malicious file, or executes an existing file that has been misconfigured to allow executable access to the adversary.

Prerequisites

System's configuration must allow an attacker to directly access executable files or upload files to execute. This means that any access control system that is supposed to mediate communications between the subject and the object is set incorrectly or assumes a benign environment.

Skills Required

[Level: Low]

To identify and execute against an over-privileged system interface

Resources Required

Ability to communicate synchronously or asynchronously with server that publishes an over-privileged directory, program, or interface. Optionally, ability to capture output directly through synchronous communication or other method such as FTP.

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
Confidentiality Integrity Availability	Execute Unauthorized Commands	
Integrity	Modify Data	
Confidentiality	Read Data	
Confidentiality Access Control Authorization	Gain Privileges	

Mitigations

Design: Enforce principle of least privilege
Design: Run server interfaces with a non-root account and/or utilize chroot jails or other configuration techniques to constrain privileges even if attacker gains some limited access to commands.
Implementation: Perform testing such as pen-testing and vulnerability scanning to identify directories, programs, and interfaces that grant direct access to executables.

Example Instances

Consider a directory on a web server with the following permissions

drwxrwxrwx 5 admin public 170 Nov 17 01:08 webroot

This could allow an attacker to both execute and upload and execute programs' on the web server. This one vulnerability can be exploited by a threat to probe the system and identify additional vulnerabilities to exploit.

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
1574.005	Hijack Execution Flow: Executable Installer File Permissions Weakness
1574.010	Hijack Execution Flow: Services File Permissions Weakness

References

[REF-1] G. Hoglund and G. McGraw. "Exploiting Software: How to Break Code". Addison-Wesley. 2004-02.

Content History

Submissions		
Submission Date	Submitter	Organization

2014-06-23 (Version 2.6)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**
2015-12-07 (Version 2.8)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Attack_Patterns	
2017-05-01 (Version 2.10)	CAPEC Content Team	The MITRE Corporation
	Updated References	
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Attack_Patterns, Taxonomy_Mappings	
2020-12-17 (Version 3.4)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Attack_Patterns	
2021-06-24 (Version 3.5)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Weaknesses	
2022-02-22 (Version 3.7)	CAPEC Content Team	The MITRE Corporation
	Updated Description, Execution_Flow	
2022-09-29 (Version 3.8)	CAPEC Content Team	The MITRE Corporation
	Updated Example_Instances, Related_Attack_Patterns, Taxonomy_Mappings	
Previous Entry Names		
Change Date	**Previous Entry Name**	
2018-07-31 (Version 2.12)	Accessing, Modifying or Executing Executable Files	

More information is available — Please select a different filter.
