CAPEC-471: Search Order Hijacking (Version 3.9)

Archived: 2026-04-05 21:22:58 UTC

CAPEC

Common Attack Pattern Enumeration and Classification

A Community Resource for Identifying and Understanding Attacks

New to CAPEC? Start Here!

Attack Pattern ID: 471

Abstraction: Detailed

Description

An adversary exploits a weakness in an application's specification of external libraries to exploit the functionality of the loader where the process loa different libraries and with many different loading processes. No forensic trails are left in the system's registry or file system that an incorrect library

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 ChildO

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 att

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

View Name
Domains of Attack
Mechanisms of Attack

Execution Flow

Explore

1. **Identify target general susceptibility:** An attacker uses an automated tool or manually finds whether the target application uses dynamically

Techniques
The attacker uses a tool such as the OSX "otool" utility or manually probes whether the target application uses dynamically linked libraries
The attacker finds the configuration files containing the entries to the dynamically linked libraries and modifies the entries to point to the m

Experiment

1. **Craft malicious libraries:** The attacker uses knowledge gained in the Explore phase to craft malicious libraries that they will redirect the tar

Techniques
The attacker monitors the file operations performed by the target application using a tool like dtrace or FileMon. And the attacker can delay

Exploit

1. **Redirect the access to libraries to the malicious libraries:** The attacker redirects the target to the malicious libraries they crafted in the Exp

Techniques
The attacker modifies the entries in the configuration files pointing to the malicious libraries they crafted.
The attacker leverages symlink/timing issues to redirect the target to access the malicious libraries they crafted. See also: CAPEC-132.
The attacker leverages file search path order issues to redirect the target to access the malicious libraries they crafted. See also: CAPEC-38.

Prerequisites

Attacker has a mechanism to place its malicious libraries in the needed location on the file system.

Skills Required

[Level: Medium]

Ability to create a malicious library.

Mitigations

Design: Fix the Windows loading process to eliminate the preferential search order by looking for DLLs in the precise location where they are exp
Design: Sign system DLLs so that unauthorized DLLs can be detected.

Example Instances

For instance, an attacker with access to the file system may place a malicious ntshrui.dll in the C:\Windows directory. This DLL normally resides i loading explorer.exe process, the DLL supplied by the attacker will be found first and thus loaded in lieu of the legitimate DLL. Since explorer.exe
macOS and OS X use a common method to look for required dynamic libraries (dylib) to load into a program based on search paths. Adversaries c the program is configured to run at a higher privilege level than the current user, then when the dylib is loaded into the application, the dylib will a

Taxonomy Mappings

CAPEC mappings to ATT&CK techniques leverage an inheritance model to streamline and minimize direct CAPEC/ATT&CK mappings. Inherit

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

Entry ID	Entry Name
1574.001	Hijack Execution Flow:DLL search order hijacking
1574.004	Hijack Execution Flow: Dylib Hijacking
1574.008	Hijack Execution Flow: Path Interception by Search Order Hijacking

References

[REF-409] "M Trends Report". Mandiant. 2011. <https://www.mandiant.com>.

Content History

Submissions	
Submission Date	**Submitter**
2014-06-23 (Version 2.6)	CAPEC Content Team
Modifications	

Modification Date	Modifier
2015-11-09 (Version 2.7)	CAPEC Content Team
	Updated References
2018-07-31 (Version 2.12)	CAPEC Content Team
	Updated Attack_Phases, Attack_Prerequisites, Attacker_Skills_or_Knowledge_Required, Des
2019-04-04 (Version 3.1)	CAPEC Content Team
	Updated Taxonomy_Mappings
2020-07-30 (Version 3.3)	CAPEC Content Team
	Updated Execution_Flow, Taxonomy_Mappings
2020-12-17 (Version 3.4)	CAPEC Content Team
	Updated Mitigations
2021-06-24 (Version 3.5)	CAPEC Content Team
	Updated Taxonomy_Mappings
2022-09-29 (Version 3.8)	CAPEC Content Team
	Updated Taxonomy_Mappings

Previous Entry Names

Change Date	Previous Entry Name
2018-07-31 (Version 2.12)	DLL Search Order Hijacking

More information is available — Please select a different filter.

Page Last Updated or Reviewed: July 31, 2018

Source: https://capec.mitre.org/data/definitions/471.html