CAPEC-641: DLL Side-Loading (Version 3.9)

Archived: 2026-04-05 14:20:49 UTC

Description

An adversary places a malicious version of a Dynamic-Link Library (DLL) in the Windows Side-by-Side (WinSxS) directory to trick the operating system into loading this malicious DLL instead of a legitimate DLL. Programs specify the location of the DLLs to load via the use of WinSxS manifests or DLL redirection and if they aren't used then Windows searches in a predefined set of directories to locate the file. If the applications improperly specify a required DLL or WinSxS manifests aren't explicit about the characteristics of the DLL to be loaded, they can be vulnerable to side-loading.

Likelihood Of Attack

Typical Severity

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.

Prerequisites

The target must fail to verify the integrity of the DLL before using them.

Skills Required

[Level: High]

Trick the operating system in loading a malicious DLL instead of a legitimate DLL.

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 Bypass Protection Mechanism	

Mitigations

Prevent unknown DLLs from loading through using an allowlist policy.
Patch installed applications as soon as new updates become available.
Properly restrict the location of the software being used.
Use of sxstrace.exe on Windows as well as manual inspection of the manifests.
Require code signing and avoid using relative paths for resources.

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
1574.002	Hijack Execution Flow:DLL Side-Loading

References

Content History

Submissions		
Submission Date	**Submitter**	**Organization**
2018-07-31 (Version 2.12)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**
2019-04-04 (Version 3.1)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Mitigations, Taxonomy_Mappings	

More information is available — Please select a different filter.

Source: https://capec.mitre.org/data/definitions/641.html