CAPEC-579: Replace Winlogon Helper DLL (Version 3.9)

Archived: 2026-04-06 01:30:12 UTC

Attack Pattern ID: 579 **Abstraction: Detailed**		

Description

Winlogon is a part of Windows that performs logon actions. In Windows systems prior to Windows Vista, a registry key can be modified that causes Winlogon to load a DLL on startup. Adversaries may take advantage of this feature to load adversarial code at startup.

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

Mitigations

Changes to registry entries in "HKLM\Software\Microsoft\Windows NT\Winlogon\Notify" that do not correlate with known software, patch cycles, etc are suspicious. New DLLs written to System32 which do not correlate with known good software or patching may be suspicious.

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
1547.004	Boot or Logon Autostart Execution: Winlogon helper DLL

Content History

Submissions		
Submission Date	**Submitter**	**Organization**
2015-11-09 (Version 2.7)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**

2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	
2023-01-24 (Version 3.9)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Weaknesses	

More information is available — Please select a different filter.
