CAPEC-639: Probe System Files (Version 3.9)

Archived: 2026-04-05 21:33:40 UTC

Attack Pattern ID: 639 **Abstraction: Detailed**		

Description

An adversary obtains unauthorized information due to improperly protected files. If an application stores sensitive information in a file that is not protected by proper access control, then an adversary can access the file and search for sensitive information.

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 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	Collect and Analyze Information

Prerequisites

An adversary has access to the file system of a system.

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	Read Data	

Mitigations

Verify that files have proper access controls set, and reduce the storage of sensitive information to only what is necessary.

Example Instances

Adversaries may search local file systems and remote file shares for files containing passwords. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

Adversaries may search network shares on computers they have compromised to find files of interest.

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
1039	Data from Network Shared Drive
1552.001	Unsecured Credentials: Credentials in Files
1552.003	Unsecured Credentials: Bash History
1552.004	Unsecured Credentials: Private Keys
1552.006	Unsecured Credentials: Group Policy Preferences

Content History

Submissions		
Submission Date	**Submitter**	**Organization**
2018-05-04 (Version 2.11)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Attack_Patterns, 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.
