CAPEC-572: Artificially Inflate File Sizes (Version 3.9)

Archived: 2026-04-05 17:07:28 UTC

Description

An adversary modifies file contents by adding data to files for several reasons. Many different attacks could “follow” this pattern resulting in numerous outcomes. Adding data to a file could also result in a Denial of Service condition for devices with limited storage capacity.

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.

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

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
Availability	Resource Consumption	
Integrity	Modify Data	

Example Instances

An adversary could potentially increase file sizes on devices containing limited storage resources, such as SCADA or IOT devices, resulting in denial of service conditions.

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
1027.001	Obfuscated Files or Information:Binary Padding

Content History

Submissions		
Submission Date	**Submitter**	**Organization**
2015-11-09 (Version 2.7)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**
2019-04-04 (Version 3.1)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Attack_Patterns	
2019-09-30 (Version 3.2)	CAPEC Content Team	The MITRE Corporation
	Updated @Abstraction, Related_Attack_Patterns	
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Consequences, Description, Example_Instances, Likelihood_Of_Attack, Taxonomy_Mappings, Typical_Severity	
2021-06-24 (Version 3.5)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Attack_Patterns	

More information is available — Please select a different filter.
