CAPEC-187: Malicious Automated Software Update via Redirection (Version 3.9)

Archived: 2026-04-05 18:53:18 UTC

Description

An attacker exploits two layers of weaknesses in server or client software for automated update mechanisms to undermine the integrity of the target code-base. The first weakness involves a failure to properly authenticate a server as a source of update or patch content. This type of weakness typically results from authentication mechanisms which can be defeated, allowing a hostile server to satisfy the criteria that establish a trust relationship. The second weakness is a systemic failure to validate the identity and integrity of code downloaded from a remote location, hence the inability to distinguish malicious code from a legitimate update.

Extended Description

One predominate type of redirection attack requires DNS spoofing or hijacking of a domain name corresponding to an update server. The target software initiates an update request and the DNS request resolves the domain name of the update server to the IP address of the attacker, at which point the software accepts updates either transmitted by or pulled from the attackers' server. Attacks against DNS mechanisms comprise an initial phase of a chain of attacks that facilitate automated update hijacking attack, and such attacks have a precedent in targeted activities that have been as complex as DNS/BIND attacks of corporate infrastructures, to untargeted attacks aimed at compromising home broadband routers, as well as attacks involving the compromise of wireless access points, as well as 'evil twin' attacks coupled with DNS redirection. Due to the plethora of options open to the attacker in forcing name resolution to arbitrary servers the Automated Update Hijacking attack strategies are the tip of the spear for many multi-stage attack chains.

The second weakness that is exploited by the attacker is the lack of integrity checking by the software in validating the update. Software which relies only upon domain name resolution to establish the identity of update code is particularly vulnerable, because this signals an absence of other security countermeasures that could be applied to invalidate the attackers' payload on basis of code identity, hashing, signing, encryption, and other integrity checking mechanisms. Redirection-based attack patterns work equally well against client-side software as well as local servers or daemons that provide software update functionality.

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.

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
Access Control Availability	Execute Unauthorized Commands	

Confidentiality		

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
1072	Software Deployment Tools

Content History

Submissions		
Submission Date	**Submitter**	**Organization**
2014-06-23 (Version 2.6)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**
2015-11-09 (Version 2.7)	CAPEC Content Team	The MITRE Corporation
	Updated Activation_Zone, Architectural_Paradigms, Injection_Vector, Payload, Payload_Activation_Impact, References, Technical_Context	
2017-08-04 (Version 2.11)	CAPEC Content Team	The MITRE Corporation
	Updated Resources_Required	
2019-09-30 (Version 3.2)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Attack_Patterns	
2020-12-17 (Version 3.4)	CAPEC Content Team	The MITRE Corporation
	Updated @Name, Consequences, Description, Likelihood_Of_Attack, Taxonomy_Mappings	
2022-02-22 (Version 3.7)	CAPEC Content Team	The MITRE Corporation
	Updated Description, Extended_Description	
Previous Entry Names		
Change Date	**Previous Entry Name**	
2020-12-17 (Version 3.4)	Malicious Automated Software Update	

More information is available — Please select a different filter.