CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')

Weakness ID: 757
Vulnerability Mapping: ALLOWED
Abstraction: Base

View customized information: Conceptual | Operational | Mapping Friendly | **Complete** | Custom

Description

A protocol or its implementation supports interaction between multiple actors and allows those actors to negotiate which algorithm should be used as a protection mechanism such as encryption or authentication, but it does not select the strongest algorithm that is available to both parties.

Extended Description

When a security mechanism can be forced to downgrade to use a less secure algorithm, this can make it easier for attackers to compromise the product by exploiting weaker algorithm. The victim might not be aware that the less secure algorithm is being used. For example, if an attacker can force a communications channel to use cleartext instead of strongly-encrypted data, then the attacker could read the channel by sniffing, instead of going through extra effort of trying to decrypt the data using brute force techniques.

Common Consequences

Scope	Impact	Likelihood
Access Control	**Technical Impact:** *Bypass Protection Mechanism*	

Relationships

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
ChildOf	P	693	Protection Mechanism Failure
PeerOf	B	1328	Security Version Number Mutable to Older Versions

Relevant to the view "Architectural Concepts" (CWE-1008)

Modes Of Introduction

Phase	Note
Architecture and Design	COMMISSION: This weakness refers to an incorrect design related to an architectural security tactic.

Observed Examples

Reference	Description
CVE-2006-4302	Attacker can select an older version of the software to exploit its vulnerabilities.
CVE-2006-4407	Improper prioritization of encryption ciphers during negotiation leads to use of a weaker cipher.
CVE-2005-2969	chain: SSL/TLS implementation disables a verification step (CWE-325) that enables a downgrade attack to a weaker protocol.
CVE-2001-1444	Telnet protocol implementation allows downgrade to weaker authentication and encryption using an Adversary-in-the-Middle AITM attack.
CVE-2002-1646	SSH server implementation allows override of configuration setting to use weaker authentication schemes. This may be a composite with CWE-642.

Detection Methods

Automated Static Analysis

Automated static analysis, commonly referred to as Static Application Security Testing (SAST), can find some instances of this weakness by analyzing source code (or binary/compiled code) without having to execute it. Typically, this is done by building a model of data flow and control flow, then searching for potentially-vulnerable patterns that connect "sources" (origins of input) with "sinks" (destinations where the data interacts with external components, a lower layer such as the OS, etc.)

Effectiveness: High

Memberships

Nature	Type	ID	Name
MemberOf	C	957	SFP Secondary Cluster: Protocol Error
MemberOf	C	1346	OWASP Top Ten 2021 Category A02:2021 - Cryptographic Failures
MemberOf	C	1413	Comprehensive Categorization: Protection Mechanism Failure

Vulnerability Mapping Notes

Usage: ALLOWED *(this CWE ID could be used to map to real-world vulnerabilities)*

Reason: Acceptable-Use

Rationale:

This CWE entry is at the Base level of abstraction, which is a preferred level of abstraction for mapping to the root causes of vulnerabilities.

Comments:

Carefully read both the name and description to ensure that this mapping is an appropriate fit. Do not try to 'force' a mapping to a lower-level Base/Variant simply to comply with this preferred level of abstraction.

Notes

Relationship

This is related to CWE-300, although not all downgrade attacks necessarily require an entity that redirects or interferes with the network. See examples.

Related Attack Patterns

CAPEC-ID	Attack Pattern Name
CAPEC-220	Client-Server Protocol Manipulation
CAPEC-606	Weakening of Cellular Encryption
CAPEC-620	Drop Encryption Level

Content History

Submissions

Submission Date	Submitter	Organization
2009-03-03 *(CWE 1.3, 2009-03-10)*	CWE Content Team	MITRE

Modifications

Page Last Updated: July 16, 2024