# CWE Detail – CWE-757

## 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.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** 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.

## Related Attack Patterns (CAPEC)

* CAPEC-220
* CAPEC-606
* CAPEC-620

## Attack TTPs

**•** T1600: Weaken Encryption (Tactics: defense-evasion)

## Modes of Introduction

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

## Common Consequences

**•** Impact: Bypass Protection Mechanism — Notes:

## 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.