# CWE Detail – CWE-347

## Description

The product does not verify, or incorrectly verifies, the cryptographic signature for data.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-1796: Does not properly verify signatures for "trusted" entities.

**•** CVE-2005-2181: Insufficient verification allows spoofing.

**•** CVE-2005-2182: Insufficient verification allows spoofing.

**•** CVE-2002-1706: Accepts a configuration file without a Message Integrity Check (MIC) signature.

## Related Attack Patterns (CAPEC)

* CAPEC-463
* CAPEC-475

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity, Modify Application Data, Execute Unauthorized Code or Commands — Notes: An attacker could gain access to sensitive data and possibly execute unauthorized code.

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** The JAR file that was potentially downloaded from an untrusted source is created without verifying the signature (if present). An alternate constructor that accepts a boolean verify parameter should be used instead.