# CWE Detail – CWE-422

## Description

The product does not properly verify the source of a message in the Windows Messaging System while running at elevated privileges, creating an alternate channel through which an attacker can directly send a message to the product.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2002-0971: Bypass GUI and access restricted dialog box.

**•** CVE-2002-1230: Gain privileges via Windows message.

**•** CVE-2003-0350: A control allows a change to a pointer for a callback function using Windows message.

**•** CVE-2003-0908: Product launches Help functionality while running with raised privileges, allowing command execution using Windows message to access "open file" dialog.

**•** CVE-2004-0213: Attacker uses Shatter attack to bypass GUI-enforced protection for CVE-2003-0908.

**•** CVE-2004-0207: User can call certain API functions to modify certain properties of privileged programs.

## Modes of Introduction

**•** Architecture and Design: N/A

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Architecture and Design: Always verify and authenticate the source of the message. (Effectiveness: N/A)

## Applicable Platforms

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

## Notes

**•** Relationship: Overlaps privilege errors and UI errors.

**•** Research Gap: Possibly under-reported, probably under-studied. It is suspected that a number of publicized vulnerabilities that involve local privilege escalation on Windows systems may be related to Shatter attacks, but they are not labeled as such. Alternate channel attacks likely exist in other operating systems and messaging models, e.g. in privileged X Windows applications, but examples are not readily available.