# CWE Detail – CWE-360

## Description

Security based on event locations are insecure and can be spoofed.

## Extended Description

Events are a messaging system which may provide control data to programs listening for events. Events often do not have any type of authentication framework to allow them to be verified from a trusted source. Any application, in Windows, on a given desktop can send a message to any window on the same desktop. There is no authentication framework for these messages. Therefore, any message can be used to manipulate any process on the desktop if the process does not check the validity and safeness of those messages.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

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

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity, Execute Unauthorized Code or Commands — Notes: If one trusts the system-event information and executes commands based on it, one could potentially take actions based on a spoofed identity.

## Potential Mitigations

**•** Architecture and Design: Never trust or rely any of the information in an Event for security. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** This code does not attempt to prevent unauthorized users from activating the button. Even if the button is rendered non-functional to unauthorized users in the application UI, an attacker can easily send a false button press event to the application window and expose the secret information.