# CWE Detail – CWE-356

## Description

The product's user interface does not warn the user before undertaking an unsafe action on behalf of that user. This makes it easier for attackers to trick users into inflicting damage to their system.

## Extended Description

Product systems should warn users that a potentially dangerous action may occur if the user proceeds. For example, if the user downloads a file from an unknown source and attempts to execute the file on their machine, then the application's GUI can indicate that the file is unsafe.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-1999-1055: Product does not warn user when document contains certain dangerous functions or macros.

**•** CVE-1999-0794: Product does not warn user when document contains certain dangerous functions or macros.

**•** CVE-2000-0277: Product does not warn user when document contains certain dangerous functions or macros.

**•** CVE-2000-0517: Product does not warn user about a certificate if it has already been accepted for a different site. Possibly resultant.

**•** CVE-2005-0602: File extractor does not warn user if setuid/setgid files could be extracted. Overlaps privileges/permissions.

**•** CVE-2000-0342: E-mail client allows bypass of warning for dangerous attachments via a Windows .LNK file that refers to the attachment.

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Hide Activities — Notes:

## Applicable Platforms

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

## Notes

**•** Relationship: Often resultant, e.g. in unhandled error conditions.

**•** Relationship: Can overlap privilege errors, conceptually at least.