# CWE Detail – CWE-623

## Description

An ActiveX control is intended for restricted use, but it has been marked as safe-for-scripting.

## Extended Description

This might allow attackers to use dangerous functionality via a web page that accesses the control, which can lead to different resultant vulnerabilities, depending on the control's behavior.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2007-0617: control allows attackers to add malicious email addresses to bypass spam limits

**•** CVE-2007-0219: web browser uses certain COM objects as ActiveX

**•** CVE-2006-6510: kiosk allows bypass to read files

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Execute Unauthorized Code or Commands — Notes:

## Potential Mitigations

**•** Architecture and Design: During development, do not mark it as safe for scripting. (Effectiveness: N/A)

**•** System Configuration: After distribution, you can set the kill bit for the control so that it is not accessible from Internet Explorer. (Effectiveness: N/A)