# CWE Detail – CWE-618

## Description

An ActiveX control is intended for use in a web browser, but it exposes dangerous methods that perform actions that are outside of the browser's security model (e.g. the zone or domain).

## Extended Description

ActiveX controls can exercise far greater control over the operating system than typical Java or javascript. Exposed methods can be subject to various vulnerabilities, depending on the implemented behaviors of those methods, and whether input validation is performed on the provided arguments. If there is no integrity checking or origin validation, this method could be invoked by attackers.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2007-1120: download a file to arbitrary folders.

**•** CVE-2006-6838: control downloads and executes a url in a parameter

**•** CVE-2007-0321: resultant buffer overflow

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Other — Notes:

## Potential Mitigations

**•** Implementation: If you must expose a method, make sure to perform input validation on all arguments, and protect against all possible vulnerabilities. (Effectiveness: N/A)

**•** Architecture and Design: Use code signing, although this does not protect against any weaknesses that are already in the control. (Effectiveness: N/A)

**•** Architecture and Design: Where possible, avoid marking the control as safe for scripting. (Effectiveness: N/A)