# CWE Detail – CWE-368

## Description

A product performs a series of non-atomic actions to switch between contexts that cross privilege or other security boundaries, but a race condition allows an attacker to modify or misrepresent the product's behavior during the switch.

## Extended Description

This is commonly seen in web browser vulnerabilities in which the attacker can perform certain actions while the browser is transitioning from a trusted to an untrusted domain, or vice versa, and the browser performs the actions on one domain using the trust level and resources of the other domain.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2009-1837: Chain: race condition (CWE-362) from improper handling of a page transition in web client while an applet is loading (CWE-368) leads to use after free (CWE-416)

**•** CVE-2004-2260: Browser updates address bar as soon as user clicks on a link instead of when the page has loaded, allowing spoofing by redirecting to another page using onUnload method. \*\* this is one example of the role of "hooks" and context switches, and should be captured somehow - also a race condition of sorts \*\*

**•** CVE-2004-0191: XSS when web browser executes Javascript events in the context of a new page while it's being loaded, allowing interaction with previous page in different domain.

**•** CVE-2004-2491: Web browser fills in address bar of clicked-on link before page has been loaded, and doesn't update afterward.

## Related Attack Patterns (CAPEC)

* CAPEC-26
* CAPEC-29

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Modify Application Data, Read Application Data — Notes:

## Applicable Platforms

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

## Notes

**•** Relationship: Can overlap signal handler race conditions.

**•** Research Gap: Under-studied as a concept. Frequency unknown; few vulnerability reports give enough detail to know when a context switching race condition is a factor.