# CVE Detail – CVE-2009-1837

Race condition in the NPObjWrapper\_NewResolve function in modules/plugin/base/src/nsJSNPRuntime.cpp in xul.dll in Mozilla Firefox 3 before 3.0.11 might allow remote attackers to execute arbitrary code via a page transition during Java applet loading, related to a use-after-free vulnerability for memory associated with a destroyed Java object.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.83666

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
* CWE-416: Use After Free

## CAPEC(s)

* CAPEC-26: Leveraging Race Conditions
* CAPEC-29: Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions

## Affected Products

* cpe:2.3:a:mozilla:firefox:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:9:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:4.8:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:5.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server\_aus:5.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:5.0:\*:\*:\*:\*:\*:\*:\*