# CVE Detail – CVE-2010-2753

Integer overflow in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, Thunderbird 3.0.x before 3.0.6 and 3.1.x before 3.1.1, and SeaMonkey before 2.0.6 allows remote attackers to execute arbitrary code via a large selection attribute in a XUL tree element, which triggers a use-after-free.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.88081

## CVSS Scoring

CVSS v3.1 Score: 8.8

Severity: HIGH

## Mapped CWE(s)

* CWE-190: Integer Overflow or Wraparound
* CWE-416: Use After Free

## CAPEC(s)

* CAPEC-92: Forced Integer Overflow

## Affected Products

* cpe:2.3:a:mozilla:firefox:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mozilla:firefox:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mozilla:seamonkey:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mozilla:thunderbird:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mozilla:thunderbird:3.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:11.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:11.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:11.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_desktop:11:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_desktop:11:sp1:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_server:11:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_server:11:sp1:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_software\_development\_kit:11:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_software\_development\_kit:11:sp1:\*:\*:\*:\*:\*:\*