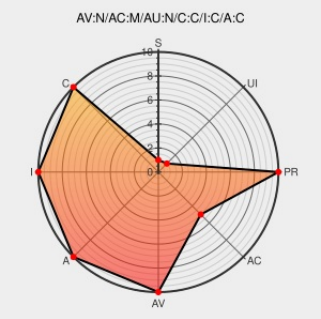
CVE-2010-1212

Published on: 07/30/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:04 PM UTC

CVE-2010-1212

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Firefox from Mozilla contain the following vulnerability:

js/src/jstracer.cpp in the browser engine in Mozilla Firefox 3.6.x before 3.6.7 and Thunderbird 3.1.x before 3.1.1 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) propagation of deep aborts in the TraceRecorder::record_JSOP_BINDNAME function, (2) depth handling in the TraceRecorder::record_JSOP_GETELEM function, and (3) tracing of out-of-range arguments in the TraceRecorder::record_JSOP_ARGSUB function.

CVE-2010-1212 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
530955 – New crash [@ ExecuteTree] in Firefox 3.6b3	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=530955
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11771
MFSA 2010-34: Miscellaneous memory safety hazards (rv:1.9.2.7/ 1.9.1.11)	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2010/mfsa2010-34.html
568855 – Crash [@ nanojit::LIns::opcode] with non-native __proto__	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=568855

558618 – TM: Crash [@ js_ValueToString] - Segfault when accessing out-of-range arguments on trace	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=558618

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	3.6.1	All	All	All
Application	Mozilla	Firefox	3.6.2	All	All	All
Application	Mozilla	Firefox	3.6.3	All	All	All
Application	Mozilla	Firefox	3.6.4	All	All	All
Application	Mozilla	Firefox	3.6.6	All	All	All
Application	Mozilla	Firefox	3.6.1	All	All	All
Application	Mozilla	Firefox	3.6.2	All	All	All
Application	Mozilla	Firefox	3.6.3	All	All	All
Application	Mozilla	Firefox	3.6.4	All	All	All
Application	Mozilla	Firefox	3.6.6	All	All	All
Application	Mozilla	Thunderbird	3.1	All	All	All
Application	Mozilla	Thunderbird	3.1	All	All	All

cpe:2.3:a:mozilla:firefox:3.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.6:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.6:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:thunderbird:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:thunderbird:3.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→