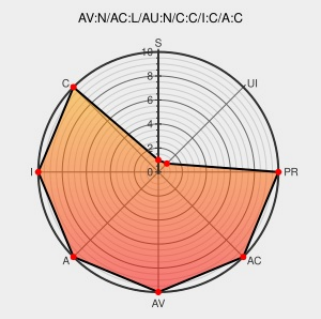
CVE-2010-2755

Published on: 07/29/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:10 PM UTC

CVE-2010-2755

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



Certain versions of Firefox from Mozilla contain the following vulnerability:

layout/generic/nsObjectFrame.cpp in Mozilla Firefox 3.6.7 does not properly free memory in the parameter array of a plugin instance, which allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted HTML document, related to the DATA and SRC attributes of an OBJECT element. NOTE: this vulnerability exists because of an incorrect fix for CVE-2010-1214.

CVE-2010-2755 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
MFSA 2010-48: Dangling pointer crash regression from plugin parameter array fix	www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2010/mfsa2010-48.html
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11961
575836 – (CVE-2010-2755) free() of garbage values when an has a |data=""| attribute and no "src" attribute --> crash [@ free | nsPluginInstanceOwner::~nsPluginInstanceOwner()]	Vendor Advisory bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=575836

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	3.6.7	All	All	All
Application	Mozilla	Firefox	3.6.7	All	All	All

cpe:2.3:a:mozilla:firefox:3.6.7:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.7:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report