



CVE-2007-6715

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2007-6715
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-04-17 22:05:00 UTC
Updated	2008-11-15 07:06:00 UTC
Description	Mozilla Firefox allows remote attackers to cause a denial of service (crash) via crafted image, as demonstrated by the zzuf

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All

References

Reference	Source	Link	Tags
44727	OSVDB	osvdb.org	
How long does it take to fix a crash-bug? - Hanno's blog	MISC	hboeck.de	
Mozilla Firefox Malformed GIF File Denial of Service Vulnerability	BID	www.securityfocus.com	
Sam Hocevar's .plan	MISC	sam.zoy.org	
zzuf - multi-purpose fuzzer	MISC	sam.zoy.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-04-22	Joshua Bressers	Red Hat does not consider this flaw a security issue. This flaw is not exploitable beyond cau

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)