



CVE-2013-1466

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

Summary

CVE	CVE-2013-1466
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-05 15:10:00 UTC
Updated	2017-08-29 01:33:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in glFusion before 1.2.2.pl4 allow remote attackers to inject arbitrary web s

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Glfusion	Glfusion	1.0.0	All	All	All
Application	Glfusion	Glfusion	1.0.0	rc1	All	All
Application	Glfusion	Glfusion	1.0.0	rc2	All	All
Application	Glfusion	Glfusion	1.0.1	All	All	All
Application	Glfusion	Glfusion	1.0.2	All	All	All
Application	Glfusion	Glfusion	1.1.0	All	All	All
Application	Glfusion	Glfusion	1.1.0	rc1	All	All
Application	Glfusion	Glfusion	1.1.1	All	All	All
Application	Glfusion	Glfusion	1.1.2	All	All	All
Application	Glfusion	Glfusion	1.1.3	All	All	All
Application	Glfusion	Glfusion	1.1.4	All	All	All
Application	Glfusion	Glfusion	1.1.4.pl1	All	All	All
Application	Glfusion	Glfusion	1.1.4.pl2	All	All	All
Application	Glfusion	Glfusion	1.1.4.pl3	All	All	All
Application	Glfusion	Glfusion	1.1.4.pl4	All	All	All
Application	Glfusion	Glfusion	1.1.5	All	All	All
Application	Glfusion	Glfusion	1.1.5.pl1	All	All	All

Application	Glfusion	Glfusion	1.1.5.pl2	All	All	All
Application	Glfusion	Glfusion	1.1.5.pl3	All	All	All
Application	Glfusion	Glfusion	1.1.6	All	All	All
Application	Glfusion	Glfusion	1.1.6.pl1	All	All	All
Application	Glfusion	Glfusion	1.1.6.pl2	All	All	All
Application	Glfusion	Glfusion	1.1.6.pl3	All	All	All
Application	Glfusion	Glfusion	1.1.6.pl4	All	All	All
Application	Glfusion	Glfusion	1.1.7	All	All	All
Application	Glfusion	Glfusion	1.1.8	All	All	All
Application	Glfusion	Glfusion	1.1.8.pl1	All	All	All
Application	Glfusion	Glfusion	1.1.8.pl2	All	All	All
Application	Glfusion	Glfusion	1.1.8.pl3	All	All	All
Application	Glfusion	Glfusion	1.1.8.pl4	All	All	All
Application	Glfusion	Glfusion	1.1.8.pl5	All	All	All
Application	Glfusion	Glfusion	1.1.8.pl6	All	All	All
Application	Glfusion	Glfusion	1.2.0	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl1	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl2	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl3	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl4	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl5	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl6	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl7	All	All	All
Application	Glfusion	Glfusion	1.2.2	All	All	All
Application	Glfusion	Glfusion	1.2.2.pl1	All	All	All
Application	Glfusion	Glfusion	1.2.2.pl2	All	All	All
Application	Glfusion	Glfusion	1.0.0	All	All	All
Application	Glfusion	Glfusion	1.0.0	rc1	All	All
Application	Glfusion	Glfusion	1.0.0	rc2	All	All
Application	Glfusion	Glfusion	1.0.1	All	All	All
Application	Glfusion	Glfusion	1.0.2	All	All	All
Application	Glfusion	Glfusion	1.1.0	All	All	All
Application	Glfusion	Glfusion	1.1.0	rc1	All	All
Application	Glfusion	Glfusion	1.1.1	All	All	All
Application	Glfusion	Glfusion	1.1.2	All	All	All

Application	Glfusion	Glfusion	1.1.3	All	All	All
Application	Glfusion	Glfusion	1.1.4	All	All	All
Application	Glfusion	Glfusion	1.1.4.pl1	All	All	All
Application	Glfusion	Glfusion	1.1.4.pl2	All	All	All
Application	Glfusion	Glfusion	1.1.4.pl3	All	All	All
Application	Glfusion	Glfusion	1.1.4.pl4	All	All	All
Application	Glfusion	Glfusion	1.1.5	All	All	All
Application	Glfusion	Glfusion	1.1.5.pl1	All	All	All
Application	Glfusion	Glfusion	1.1.5.pl2	All	All	All
Application	Glfusion	Glfusion	1.1.5.pl3	All	All	All
Application	Glfusion	Glfusion	1.1.6	All	All	All
Application	Glfusion	Glfusion	1.1.6.pl1	All	All	All
Application	Glfusion	Glfusion	1.1.6.pl2	All	All	All
Application	Glfusion	Glfusion	1.1.6.pl3	All	All	All
Application	Glfusion	Glfusion	1.1.6.pl4	All	All	All
Application	Glfusion	Glfusion	1.1.7	All	All	All
Application	Glfusion	Glfusion	1.1.8	All	All	All
Application	Glfusion	Glfusion	1.1.8.pl1	All	All	All
Application	Glfusion	Glfusion	1.1.8.pl2	All	All	All
Application	Glfusion	Glfusion	1.1.8.pl3	All	All	All
Application	Glfusion	Glfusion	1.1.8.pl4	All	All	All
Application	Glfusion	Glfusion	1.1.8.pl5	All	All	All
Application	Glfusion	Glfusion	1.1.8.pl6	All	All	All
Application	Glfusion	Glfusion	1.2.0	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl1	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl2	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl3	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl4	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl5	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl6	All	All	All
Application	Glfusion	Glfusion	1.2.0.pl7	All	All	All
Application	Glfusion	Glfusion	1.2.2	All	All	All
Application	Glfusion	Glfusion	1.2.2.pl1	All	All	All
Application	Glfusion	Glfusion	1.2.2.pl2	All	All	All
Application	Glfusion	Glfusion	All	All	All	All

References		
Reference	Source	Link
20130220 Multiple Cross-Site Scripting (XSS) in glFusion	BUGTRAQ	archives.neohapsis.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
glFusion v1.2.2 Patch Level #4 Security Updates - glFusion	CONFIRM	www.glfusion.org
Security Advisory SA52255 - glFusion Multiple Cross-Site Scripting Vulnerabilities - Secunia	SECUNIA	secunia.com
glFusion 1.2.2 - Multiple XSS Vulnerabilities	EXPLOIT-DB	www.exploit-db.com
glFusion 1.2.2 Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecurity.com
File Not Found	MISC	www.htbridge.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
No vendor comments have been submitted for this CVE.		
There are currently no legacy QID mappings associated with this CVE.		

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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