



CVE-2012-0974

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

Summary

CVE	CVE-2012-0974
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-09-25 23:55:00 UTC
Updated	2012-10-15 04:00:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the getParam function in oc-includes/osclass/core/Params.php in OSClass

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Juan Ramon	Osclass	1.1	All	All	All
Application	Juan Ramon	Osclass	1.1	rc	All	All
Application	Juan Ramon	Osclass	1.2	alpha	All	All
Application	Juan Ramon	Osclass	1.2	beta	All	All
Application	Juan Ramon	Osclass	1.2	delta	All	All
Application	Juan Ramon	Osclass	2.0	All	All	All
Application	Juan Ramon	Osclass	2.0	rc	All	All
Application	Juan Ramon	Osclass	2.0.1	All	All	All
Application	Juan Ramon	Osclass	2.0.2	All	All	All
Application	Juan Ramon	Osclass	2.0.3	All	All	All
Application	Juan Ramon	Osclass	2.1	All	All	All
Application	Juan Ramon	Osclass	2.1.1	All	All	All
Application	Juan Ramon	Osclass	2.2	All	All	All
Application	Juan Ramon	Osclass	2.2.1	All	All	All
Application	Juan Ramon	Osclass	2.2.2	All	All	All
Application	Juan Ramon	Osclass	2.2.3	All	All	All
Application	Juan Ramon	Osclass	2.3	All	All	All

Application	Juan Ramon	Osclass	2.3.1	All	All	All
Application	Juan Ramon	Osclass	2.3.2	All	All	All
Application	Juan Ramon	Osclass	2.3.3	All	All	All
Application	Juan Ramon	Osclass	1.1	All	All	All
Application	Juan Ramon	Osclass	1.1	rc	All	All
Application	Juan Ramon	Osclass	1.2	alpha	All	All
Application	Juan Ramon	Osclass	1.2	beta	All	All
Application	Juan Ramon	Osclass	1.2	delta	All	All
Application	Juan Ramon	Osclass	2.0	All	All	All
Application	Juan Ramon	Osclass	2.0	rc	All	All
Application	Juan Ramon	Osclass	2.0.1	All	All	All
Application	Juan Ramon	Osclass	2.0.2	All	All	All
Application	Juan Ramon	Osclass	2.0.3	All	All	All
Application	Juan Ramon	Osclass	2.1	All	All	All
Application	Juan Ramon	Osclass	2.1.1	All	All	All
Application	Juan Ramon	Osclass	2.2	All	All	All
Application	Juan Ramon	Osclass	2.2.1	All	All	All
Application	Juan Ramon	Osclass	2.2.2	All	All	All
Application	Juan Ramon	Osclass	2.2.3	All	All	All
Application	Juan Ramon	Osclass	2.3	All	All	All
Application	Juan Ramon	Osclass	2.3.1	All	All	All
Application	Juan Ramon	Osclass	2.3.2	All	All	All
Application	Juan Ramon	Osclass	2.3.3	All	All	All
Application	Juan Ramon	Osclass	All	All	All	All

References						
Reference	Source					
About Secunia Research Flexera	SEC					
OSClass 2.3.5 · osclass/Osclass@ff7ef8a · GitHub	COM					
NEOHAPSIS - Peace of Mind Through Integrity and Insight	BUG					
High-Tech Bridge SA - Advisories - Multiple vulnerabilities in OSClass	MISC					
OSClass SQL Injection and Cross Site Scripting Vulnerabilities	BID					
OSClass 2.3.5 Blog Osclass the free scripts classifiedBlog Osclass the free scripts classified Professional open source classifieds	COM					
CVE Program record	CVE					
NVD vulnerability detail	NVD					

No vendor comments have been submitted for this CVE.

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](#)