



CVE-2006-4608

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

Summary

CVE	CVE-2006-4608
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-07 00:04:00 UTC
Updated	2018-10-17 21:38:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in Longino Jacome php-Revista 1.1.2 allow remote attackers to inject arbit

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Longino	Jacome Php-revista	1.1.2	All	All	All
Application	Longino	Jacome Php-revista	1.1.2	All	All	All

References

Reference	Source
SecurityFocus	BUGTRAQ
Revista Multiple Input Validation Vulnerabilities	BID
28450	OSVDB
PHP-revista 1.1.2 - Remote File Inclusion / SQL Injection / Authentication Bypass / Cross-Site Scripting - PHP webapps Exploit	EXPLOIT-D
SecurityReason - PHP-Revista Multiple vulnerabilities	SREASON
SecurityFocus	BUGTRAQ
[VIM] PHP-Revista 1.1.2 (RFI/SQLi/CB/XSS) Multiple Remote Vulnerabilities	VIM
php-revista Multiple Vulnerabilities - Advisories - Secunia	SECUNIA
CVE Program record	CVE.ORG
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](#)