



CVE-2018-12229

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

Summary

CVE	CVE-2018-12229
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-12 11:29:00 UTC
Updated	2018-08-08 18:32:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Public Knowledge Project (PKP) Open Journal System (OJS) 3.0.0 to 3.1.1-1 allo

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sfu	Open Journal System	All	All	All	All

References

Reference	Source	Link	Tags
XSS vulnerability alert - PKP Announcements - PKP Community Forum	CONFIRM	forum.pkp.sfu.ca	Vendor Adviso
OJS 3.1.1-2 and OMP 3.1.1-3 Released - PKP Announcements - PKP Community Forum	CONFIRM	forum.pkp.sfu.ca	Vendor Adviso
Correct missing escaping of template variable · Issue #3785 · pkp/pkp-lib · GitHub	MISC	github.com	Third Party Ad
metamorfosec.com/Files/Advisories/METS-2018-001-A_XSS_Vulnerability_in_OJS_3.0...	MISC	metamorfosec.com	Third Party Ad
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

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

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