

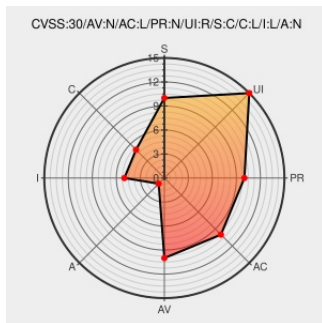


CVE-2018-12588

Published on: 06/19/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:22 PM UTC

CVE-2018-12588

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Open Monograph Press](#) from [Public Knowledge Project](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in templates/frontend/pages/searchResults.tpl in Public Knowledge Project (PKP) Open Monograph Press (OMP) v1.2.0 through 3.1.1-2 before 3.1.1-3 allows remote attackers to inject arbitrary web script or HTML via the catalog.noTitlesSearch parameter (aka the Search field).

CVE-2018-12588 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
XSS vulnerability alert - PKP Announcements - PKP Community Forum	Vendor Advisory forum.pkp.sfu.ca text/html	PKP CONFIRM forum.pkp.sfu.ca/t/xss-vulnerability-alert/45938

OJS 3.1.1-2 and OMP 3.1.1-3 Released - PKP Announcements - PKP Community Forum	Exploit Patch Vendor Advisory forum.pkp.sfu.ca text/html	PKP CONFIRM forum.pkp.sfu.ca/t/ojs-3-1-1-2-and-omp-3-1-1-3-released/45937
Correct missing escaping in searchResults.tpl · Issue #3805 · pkp/pkp-lib · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/pkp/pkp-lib/issues/3805
No Description Provided	Technical Description Third Party Advisory metamorfosec.com text/html	MISC metamorfosec.com/Files/Advisories/METS-2018-002-A_XSS_Vulnerability_in_OMP_1.2.0_to_3.1.1-2.txt
pkp/pkp-lib#3805 Add missing escaping to catalog.noTitlesSearch · pkp/omp@bfdcdec · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/pkp/omp/commit/bfdcdec64865238163282c5940a6c7896c0977bf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Public Knowledge Project	Open Monograph Press	All	All	All	All
Application	Public Knowledge Project	Open Monograph Press	All	All	All	All
cpe:2.3:a:public_knowledge_project:open_monograph_press:*****:						
cpe:2.3:a:public_knowledge_project:open_monograph_press:*****:						

No vendor comments have been submitted for this CVE