



CVE-2018-6378

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2018-6378 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-05-22 15:29:00 UTC |
| Updated | 2018-06-22 17:21:00 UTC |
| Description | In Joomla! Core before 3.8.8, inadequate filtering of file and folder names leads to various XSS attack vectors in the media |

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|------------------------|---------|---------|--------|---------|----------|
| Application | Joomla | Joomla! | All | All | All | All |
| Application | Joomla | Joomla! | All | All | All | All |
| Application | Joomla | Joomla! | All | All | All | All |

References

Reference

[20180509] - Core - XSS vulnerability in the media manager

Joomla! Core CVE-2018-6378 Cross Site Scripting Vulnerability

Joomla! Multiple Flaws Let Remote Authenticated Users Modify ACLs and Execute Arbitrary Code, Remote Users Obtain Potentially Sensitive

CVE Program record

NVD vulnerability detail

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](#)