



CVE-2017-6814

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

Summary

CVE	CVE-2017-6814
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-12 01:59:00 UTC
Updated	2019-03-19 13:24:00 UTC
Description	In WordPress before 4.7.3, there is authenticated Cross-Site Scripting (XSS) via Media File Metadata. This is demonstrated

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

References

Reference

WordPress 3.6.0-4.7.2 - Authenticated Cross-Site Scripting (XSS) via Media File Metadata
oss-security - WordPress audio playlist functionality is affected by Cross-Site Scripting
Debian -- Security Information -- DSA-3815-1 wordpress
WordPress Multiple Flaws Let Remote Users Deny Service, Bypass URL Redirect Validation, Conduct Cross-Site Scripting Attacks, and Cond
WordPress 4.7.3 Security and Maintenance Release
sumofpwn.nl/advisory/2016/wordpress_audio_playlist_functionality_is_affec...
WordPress Prior to 4.7.3 Multiple Cross Site Scripting Vulnerabilities
Version 4.7.3 « WordPress Codex
Validate video and audio metadata. · WordPress/WordPress@28f838c · GitHub

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](#)