



[← To plugin page](#)


 Verified  Not fixed

WordPress MP3 jPlayer plugin <= 2.7.3 - Multiple Cross-Site Request Forgery (CSRF) vulnerabilities



CVSS 3.1 score
Medium severity








 Monitoring
Not reported to be exploited

Report 

Find out about vulnerable plugins in your websites for free.



Scan your website >

Type	Plugin
Vulnerable versions	<= 2.7.3
Fixed in	N/A
PSID 	f14e926c10bd
CVE ID 	 CVE-2022-36373
Classification 	Cross Site Request Forgery (CSRF)
OWASP Top 10 	A5: Broken Access Control
Credits	 Rasi Afeef (Patchstack Alliance)
Publicly disclosed	2022-09-01

Details

Multiple Cross-Site Request Forgery (CSRF) vulnerabilities were discovered by Rasi Afeef (Patchstack Alliance) in the WordPress MP3-jPlayer plugin (versions <= 2.7.3).








Solution

Deactivate and delete. No reply from the vendor.

References

Other known vulnerabilities for MP3 jPlayer

Full Path Disclosure	<= 2.3.3 
Local File Disclosure	<= 2.3 
Local File Disclosure	<= 2.3 
Cross Site Scripting	<= 1.8.7 
Cross Site Scripting	<= 1.8.7 

Submit vulnerabilities and become a verified Alliance member

Learn more >

\$1500

MONTHLY POOL



WordPress security

Plugin auditing

Vulnerability database

Vulnerability API

Bug bounty program **BETA**

About us

Careers

Media kit

Insights & articles



Patchstack for WordPress

For agencies **NEW**

Pricing & features

Documentation

Changelog



DPA

Privacy Policy

Terms & Conditions

