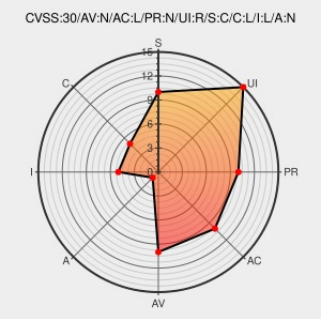
CVE-2018-5776

Published on: 01/18/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:45 PM UTC

CVE-2018-5776

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wordpress from Wordpress contain the following vulnerability:

WordPress before 4.9.2 has XSS in the Flash fallback files in MediaElement (under wp-includes/js/mediaelement).

CVE-2018-5776 has been assigned by 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
Version 4.9.2 | WordPress.org	Product, Vendor Advisory, codex.wordpress.org, text/html	CONFIRM codex.wordpress.org/Version_4.9.2

WordPress 3.7-4.9.1 - MediaElement Cross-Site Scripting (XSS)	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC wpvulndb.com/vulnerabilities/9006
External Libraries: Remove unnecessary / obsoleted MediaElement.js fi… · WordPress/WordPress@3fe9cb6 · GitHub	Patch github.com text/html	CONFIRM github.com/WordPress/WordPress/commit/3fe9cb61ee71fcfadb5e002399296
WordPress 4.9.2 Security and Maintenance Release	Release Notes Vendor Advisory wordpress.org text/html	CONFIRM wordpress.org/news/2018/01/wordpress-4-9-2-security-and-ma release/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wordpress	Wordpress	All	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→