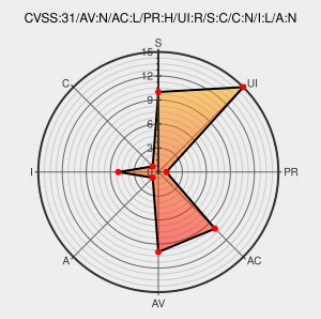
CVE-2022-30536

Published on: Not Yet Published

Last Modified on: 07/25/2022 03:33:00 AM UTC

CVE-2022-30536

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



Certain versions of Wp Maintenance from Wp Maintenance Project contain the following vulnerability:

Authenticated Stored Cross-Site Scripting (XSS) vulnerability in Florent Maillefaud's WP Maintenance plugin <= 6.0.7 at WordPress.

CVE-2022-30536 has been assigned by audit@patchstack.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Florent Maillefaud** - **WP Maintenance (WordPress plugin)** version **<= 6.0.7**

CVSS3 Score: 4.8 - MEDIUM

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

CVE References

Description	Tags	Link
WordPress WP Maintenance plugin <= 6.0.7 - Authenticated Stored Cross-Site Scripting (XSS) vulnerability - Patchstack	patchstack.com text/html	CONFIRM patchstack.com/database/vulnerability/wp-maintenance/wordpress-wp-maintenance-plugin-6-0-7-authenticated-stored-cross-site-scripting-xss-vulnerability
WP Maintenance – WordPress plugin | WordPress.org	wordpress.org text/html	CONFIRM wordpress.org/plugins/wp-maintenance/#developers

Related QID Numbers

150554 WordPress WP Maintenance Plugin: Stored Cross-Site Scripting Vulnerability (CVE-2022-30536)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wp Maintenance Project	Wp Maintenance	All	All	All	All

cpe:2.3:a:wp_maintenance_project:wp_maintenance:*:*:*:*:*:wordpress:*:*:

Discovery Credit

Vulnerability discovered by BEE-K (Patchstack)

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-30536 : Authenticated Stored Cross-Site Scripting #XSS vulnerability in Florent Maillefaud's WP Maintena… twitter.com/i/web/status/1…	2022-07-21 18:05:16
/r/netcve	CVE-2022-30536	2022-07-21 18:38:42

← Previous ID

Next ID→