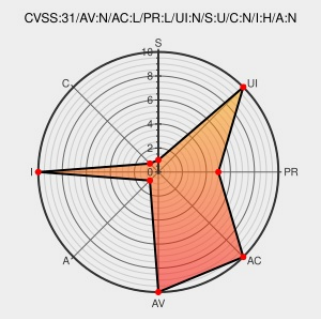
CVE-2021-24405

Published on: 07/06/2021 12:00:00 AM UTC

Last Modified on: 07/28/2022 12:17:00 PM UTC

CVE-2021-24405

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



Certain versions of Easy Cookies Policy from Izsoft contain the following vulnerability:

The Easy Cookies Policy WordPress plugin through 1.6.2 is lacking any capability and CSRF check when saving its settings, allowing any authenticated users (such as subscriber) to change them. If users can't register, this can be done through CSRF. Furthermore, the cookie banner setting is not sanitised or validated before being output in all pages of the frontend and the backend settings one, leading to a Stored Cross-Site Scripting issue.

CVE-2021-24405 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **IZSoft** - **Easy Cookies Policy** version **<= 1.6.2**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Attention Required! | Cloudflare	wpscan.com text/html Inactive Link Not Archived	CONFIRM wpscan.com/vulnerability/9157d6d2-4bda-4fcd-8192-363a63a51ff5
Internet Archive: Scheduled Maintenance	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/166543/WordPress-Easy-Cookie-Policy-1.6.2-Cross-Site-Scripting.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Izsoft	Easy Cookies Policy	All	All	All	All

cpe:2.3:a:izsoft:easy_cookies_policy:*:*:*:*:*:wordpress:*:*:

Discovery Credit

0xB9

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→