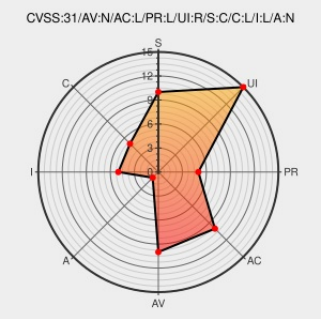
CVE-2023-2529

Published on: Not Yet Published

Last Modified on: 07/17/2023 02:18:00 PM UTC

CVE-2023-2529

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



Certain versions of Enable Svg Uploads from Enable Svg Uploads Project contain the following vulnerability:

The Enable SVG Uploads WordPress plugin through 2.1.5 does not sanitise uploaded SVG files, which could allow users with a role as low as Author to upload a malicious SVG containing XSS payloads.

CVE-2023-2529 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Unknown** - **Enable SVG Uploads** version **not down converted**

CVSS3 Score: 5.4 - MEDIUM

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

CVE References

Description	Tags	Link
Enable SVG Uploads <= 2.1.5 - Author+ Stored XSS via SVG WordPress Security Vulnerability	web.archive.org text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/4ac03907-2373-48f0-bca1-8f7073c06b18

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Enable Svg Uploads Project	Enable Svg Uploads	All	All	All	All

cpe:2.3:a:enable_svg_uploads_project:enable_svg_uploads:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-2529 : The Enable SVG Uploads WordPress plugin through 2.1.5 does not sanitise uploaded SVG files, which c… twitter.com/i/web/status/1…	2023-07-10 15:53:31

← Previous ID

Next ID→