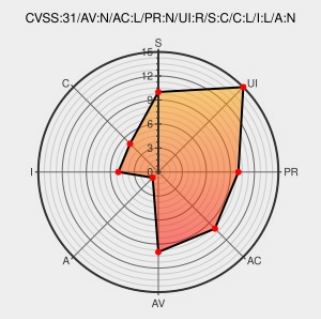
CVE-2020-29303

Published on: 12/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:10 PM UTC

CVE-2020-29303

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



Certain versions of Directories Pro from Directoriespro contain the following vulnerability:

A cross-site scripting (XSS) vulnerability in the SabaiApp Directories Pro plugin 1.3.45 for WordPress allows remote attackers to inject arbitrary web script or HTML via a POST to /wp-admin/admin.php?page=drts/directories&q=%2F with _drts_form_build_id parameter containing the XSS payload and _t_ parameter set to an invalid or non-existent CSRF token.

CVE-2020-29303 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
WordPress DirectoriesPro 1.3.45 Cross Site Scripting ≈ Packet Storm	Exploit Third Party Advisory	MISC packetstormsecurity.com/files/160452/WordPress-

	VDB Entry packetstormsecurity.com text/html	DirectoriesPro-1.3.45-Cross-Site-Scripting.html
Full Disclosure: Reflected XSS in WordPress - DirectoriesPro 1.3.45 plugin disclosure	Exploit Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20201211 Reflected XSS in WordPress - DirectoriesPro 1.3.45 plugin disclosure
Directories Pro 1.3.46 - Directories Pro	Vendor Advisory directoriespro.com text/html	CONFIRM directoriespro.com/directories-pro-1-3-46/
Advisory cve-2020-29303	Third Party Advisory www.themissinglink.com.au text/html	MISC www.themissinglink.com.au/security-advisories-cve-2020-29303

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Directoriespro	Directories Pro	1.3.45	All	All	All
Application	Directoriespro	Directories Pro	1.3.45	All	All	All

cpe:2.3:a:directoriespro:directories_pro:1.3.45:*:*:*:*:wordpress:*:*:

cpe:2.3:a:directoriespro:directories_pro:1.3.45:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→