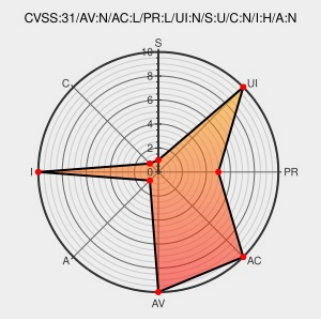
CVE-2022-28601

Published on: Not Yet Published

Last Modified on: 05/23/2022 04:29:00 PM UTC

CVE-2022-28601

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



Certain versions of 2 Factor Authentication from Lmsdoctor contain the following vulnerability:

A Two-Factor Authentication (2FA) bypass vulnerability in "Simple 2FA Plugin for Moodle" by LMS Doctor allows remote attackers to overwrite the phone number used for confirmation via the profile.php file. Therefore, allowing them to bypass the phone verification mechanism.

CVE-2022-28601 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

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
GitHub - FlaviuPopescu/CVE-2022-28601: A Two-Factor Authentication (2FA) bypass vulnerability in "Simple 2FA Plugin for Moodle" by LMS Doctor	github.com text/html	MISC github.com/FlaviuPopescu/CVE-2022-28601
Simple 2-Factor Authentication Plugin for Moodle – LMS Doctor	www.lmsdoctor.com	MISC

	text/html	www.lmsdoctor.com/simple-2-factor-authentication-plugin-for-moodle

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

Exploit/POC from Github

A Two-Factor Authentication (2FA) bypass vulnerability in "Simple 2FA Plugin for Moodle" by LMS Doctor

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lmsdoctor	2 Factor Authentication	-	All	All	All

cpe:2.3:a:lmsdoctor:2_factor_authentication:-:*:*:*:*:moodle:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@piedpiper1616	GitHub - FlaviuPopescu/CVE-2022-28601: A Two-Factor Authentication (2FA) bypass vulnerability in "Simple 2FA Plugin… twitter.com/i/web/status/1…	2022-05-09 20:33:18
@hack_git	CVE-2022-28601 A Two-Factor Authentication (2FA) bypass vulnerability in "Simple 2FA Plugin for Moodle" by LMS Doc… twitter.com/i/web/status/1…	2022-05-10 07:36:19
@Guliqbal2	#exploit 1. CVE-2022-28601: A Two-Factor Authentication bypass vulnerability in "Simple 2FA Plugin for Moodle" by L… twitter.com/i/web/status/1…	2022-05-10 11:29:01
@ksg93rd	#exploit 1. CVE-2022-28601: A Two-Factor Authentication bypass vulnerability in "Simple 2FA Plugin for Moodle" by L… twitter.com/i/web/status/1…	2022-05-10 14:57:53
@CVEreport	CVE-2022-28601 : A Two-Factor Authentication 2FA bypass vulnerability in "Simple 2FA Plugin for Moodle" by LMS Do… twitter.com/i/web/status/1…	2022-05-10 21:13:30
@phpadvisories	CVE-2022-28601 | LMS Doctor Simple 2FA Plugin auf Moodle Two-factor Authentication profile.php schwache Authentisie… twitter.com/i/web/status/1…	2022-05-11 08:13:15
/r/netcve	CVE-2022-28601	2022-05-10 22:38:39

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report