

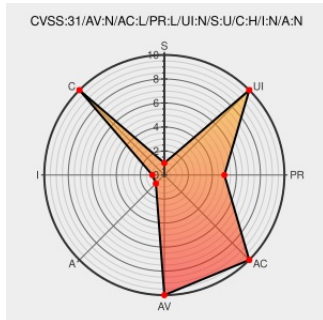


CVE-2021-25037

Published on: 01/17/2022 12:00:00 AM UTC

Last Modified on: 01/24/2022 03:12:00 PM UTC

CVE-2021-25037

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [All In One Seo](#) from [Aioseo](#) contain the following vulnerability:

The All in One SEO WordPress plugin before 4.1.5.3 is affected by an authenticated SQL injection issue, which was discovered during an internal audit by the Jetpack Scan team, and could grant attackers access to privileged information from the affected site's database (e.g., usernames and hashed passwords).

CVE-2021-25037 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Unknown - All in One SEO – Best WordPress SEO Plugin – Easily Improve SEO Rankings & Increase Traffic** version **>= 4.1.3.1**

Affected Vendor/Software: **Unknown - All in One SEO – Best WordPress SEO Plugin – Easily Improve SEO Rankings & Increase Traffic** version **< 4.1.5.3**

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	HIGH	NONE	NONE

CVSS2 Score: **4 - MEDIUM**

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

CVE References

CVE References

Description	Tags	Link
All In One SEO < 4.1.5.3 - Authenticated SQL Injection WordPress Security Vulnerability	web.archive.org text/html Inactive Link Not Archived	 MISC wpscan.com/vulnerability/4cd2a57b-3e1a-4acf-aecb-201ed9f4ee6d
Severe Vulnerabilities Fixed in All In One SEO Plugin Version 4.1.5.3	jetpack.com text/html	 MISC jetpack.com/2021/12/14/severe-vulnerabilities-fixed-in-all-in-one-seo-plugin-version-4-1-5-3/
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	 CONFIRM plugins.trac.wordpress.org/changeset/2640944/all-in-one-seo-pack/trunk/app/Common/Api/PostsTerms.php

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.

Related QID Numbers

150474 WordPress All In One SEO Plugin Multiple Vulnerabilities (CVE-2021-25036,CVE-2021-25037)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aioseo	All In One Seo	All	All	All	All
cpe:2.3:a:aioseo:all_in_one_seo:*:*:*:*:wordpress:*:*:						

Discovery Credit

Marc Montpas (Jetpack Scan)

Social Mentions

Source	Title	Posted (UTC)
 @ohhara_shiojiri	"critical Authenticated Privilege Escalation bug (CVE-2021-25036) and a high severity Authenticated SQL Injection (CVE-2021-25037)."	2021-12-22 06:19:44
 @CVEreport	CVE-2021-25037 : The All in One SEO WordPress plugin before 4.1.5.3 is affected by an authenticated SQL injection i... twitter.com/i/web/status/1...	2022-01-17 13:05:44
 @LinInfoSec	Php - CVE-2021-25037: jetpack.com/2021/12/14/sev...	2022-01-17 16:34:41
 @threatmeter	CVE-2021-25037 The All in One SEO WordPress plugin before 4.1.5.3 is affected by an authenticated SQL injection iss... twitter.com/i/web/status/1...	2022-01-18 08:09:25
 @SecRiskRptSME	RT: CVE-2021-25037 The All in One SEO WordPress plugin before 4.1.5.3 is affected by an authenticated SQL injectio... twitter.com/i/web/status/1...	2022-01-18 08:33:52
 @WesUncensored	New vulnerability on the NVD: CVE-2021-25037 ift.tt/3fvEpwq	2022-01-20 06:33:57
 @workentin	New vulnerability on the NVD: CVE-2021-25037 ift.tt/3fvEpwq	2022-01-20 06:40:35
 @xanadulinux	CVE-2021-25037 ift.tt/3fvEpwq	2022-01-20

06:52:37

 /r/netcve

[CVE-2021-25037](#)

2022-01-17

14:38:24

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)