



on the file manager, the plugin embeds monolog library which can be used to craft a gadget chain and thus trigger system command execution." />

CVE-2021-24307

Published on: 05/24/2021 12:00:00 AM UTC

Last Modified on: 05/03/2022 01:05:00 PM UTC

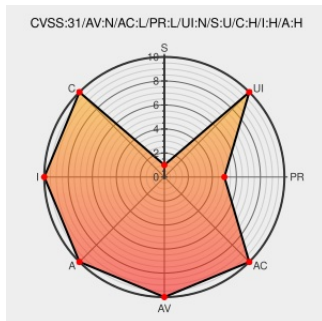
CVE-2021-24307

[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 – Best WordPress SEO Plugin – Easily Improve Your SEO Rankings before 4.1.0.2 enables authenticated users with "aioseo_tools_settings" privilege (most of the time admin) to execute arbitrary code on the underlying host. Users can restore plugin's configuration by uploading a backup .ini file in the section "Tool >

Import/Export". However, the plugin attempts to unserialize values of the .ini file. Moreover, the plugin embeds Monolog library which can be used to craft a gadget chain and thus trigger system command execution.

CVE-2021-24307 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **All in One SEO Team - All in One SEO – Best WordPress SEO Plugin – Easily Improve Your SEO Rankings** version < 4.1.0.2

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality	Integrity	Availability

Impact

COMPLETE

Impact

COMPLETE

Impact

COMPLETE

CVE References

Description

Attention Required! | Cloudflare

Tags

wpscan.com

text/html

Inactive Link

Not Archived

Link

CONFIRM

wpscan.com/vulnerability/ab2c94d2-f6c4-418b-bd14-711ed164bcf1

Description

AIOSEO Changelog - AIOSEO

Tags

aioseo.com

text/html

Link

MISC

aioseo.com/changelog/

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

Application

Vendor

Aioseo

Product

All In One Seo

Version

All

Update

All

Edition

All

Language

All

cpe:2.3:a:aioseo:all_in_one_seo:*:*:*:*:wordpress:*:*:

Discovery Credit

Vincent MICHEL

Social Mentions

Source

@CVEreport

Title

CVE-2021-24307 : The All in One SEO – Best WordPress SEO Plugin – Easily Improve Your SEO Rankings before 4.1.0.2 e... [twitter.com/i/web/status/1...](#)

Posted (UTC)

2021-05-24 11:11:24

Source

@0_exploit

Title

CVE-2021-24307 [dlvr.it/S0JGxj](#)

Posted (UTC)

2021-05-24 12:13:02

Source

/r/netcve

Title

[CVE-2021-24307](#)

Posted (UTC)

2021-05-24 11:41:45

← Previous ID

Next ID→

[site](#). This site includes MITRE data granted under the following [license](#).

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