

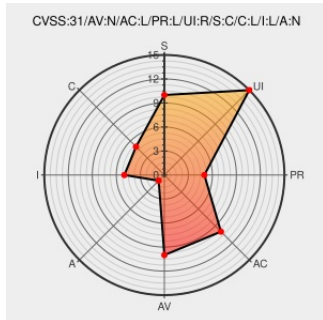


# CVE-2021-24365

Published on: 07/12/2021 12:00:00 AM UTC

Last Modified on: 07/15/2021 02:29:00 PM UTC

## CVE-2021-24365

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

Certain versions of [Admin Columns](#) from [Admincolumns](#) contain the following vulnerability:

The Admin Columns WordPress plugin Free before 4.3.2 and Pro before 5.5.2 allowed to configure individual columns for tables. Each column had a type. The type "Custom Field" allowed to choose an arbitrary database column to display in the table. There was no escaping applied to the contents of "Custom Field" columns.

CVE-2021-24365 has been assigned by [contact@wpscan.com](mailto:contact@wpscan.com) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **AdminColumns** - **Admin Columns** version < 4.3.2

Affected Vendor/Software: **AdminColumns** - **Admin Columns Pro** version < 5.5.2

CVSS3 Score: **5.4 - MEDIUM**

| Attack Vector  | Attack Complexity      | Privileges Required | User Interaction    |
|----------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b> | <b>LOW</b>             | <b>LOW</b>          | <b>REQUIRED</b>     |
| Scope          | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>CHANGED</b> | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |

CVSS2 Score: **3.5 - LOW**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>PARTIAL</b>    | <b>NONE</b>         |

## CVE References

| Description | Taas | Link |
|-------------|------|------|
|-------------|------|------|

www.syss.de

text/plain

MISC [www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-032.txt](http://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-032.txt)

wpscan.com

text/html

Inactive Link

Not Archived

CONFIRM [wpscan.com/vulnerability/fdbeb137-b404-46c7-85fb-394a3bdac388](https://wpscan.com/vulnerability/fdbeb137-b404-46c7-85fb-394a3bdac388)

Attention Required! | Cloudflare

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](mailto: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                                                    | <a href="#">Admincolumns</a> | <a href="#">Admin Columns</a> | All     | All    | All     | All      |
| Application                                                    | <a href="#">Admincolumns</a> | <a href="#">Admin Columns</a> | All     | All    | All     | All      |
| cpe:2.3:a:admincolumns:admin_columns:*:*:*:free:wordpress:*:*: |                              |                               |         |        |         |          |
| cpe:2.3:a:admincolumns:admin_columns:*:*:*:pro:wordpress:*:*:  |                              |                               |         |        |         |          |

Discovery Credit

Johannes Lauinger

SySS GmbH

| Social Mentions |                                                                                                                                                                                                          |                     |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Source          | Title                                                                                                                                                                                                    | Posted (UTC)        |
| @inj3ct0r       | #0daytoday #WordPress Admin Columns Plugin Cross Site Scripting #Vulnerability #XSS #CVE-2021-24365 <a href="#">0day.today/exploit/descr...</a>                                                          | 2021-06-23 09:10:06 |
| @AcademicoCert  | #Wordpress plugin CVE-2021-24365 Version(s):5.5.2 (Pro version), <4.3.2 (Free version) Tested Version(s):5.5.1 (Pr... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>  | 2021-06-24 12:07:12 |
| @CVEreport      | CVE-2021-24365 : The Admin Columns WordPress plugin Free before 4.3.2 and Pro before 5.5.2 allowed to configure ind... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2021-07-12 19:31:48 |
| @LinInfoSec     | Wordpress - CVE-2021-24365: <a href="https://wpscan.com/vulnerability/">wpscan.com/vulnerability/...</a>                                                                                                 | 2021-07-12 22:25:23 |
| /r/netcve       | <a href="#">CVE-2021-24365</a>                                                                                                                                                                           | 2021-07-12 19:41:11 |

[← 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](#)