

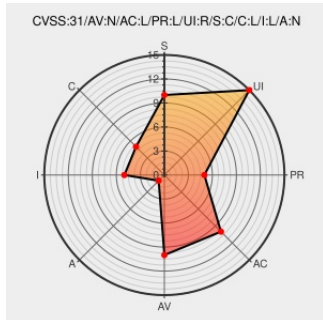


# CVE-2021-20749

Published on: 06/27/2021 12:00:00 AM UTC

Last Modified on: 07/07/2021 07:32:00 PM UTC

## CVE-2021-20749

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

Certain versions of [Fudousan Plugin](#) from [Nendeb](#) contain the following vulnerability:

Cross-site scripting vulnerability in Fudousan plugin ver5.7.0 and earlier, Fudousan Plugin Pro Single-User Type ver5.7.0 and earlier, and Fudousan Plugin Pro Multi-User Type ver5.7.0 and earlier allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.

CVE-2021-20749 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [nendeb](#) - 'Fudousan plugin' series version **Fudousan plugin ver5.7.0 and earlier, Fudousan Plugin Pro Single-User Type ver5.7.0 and earlier, and Fudousan Plugin Pro Multi-User Type ver5.7.0 and earlier**

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 | Tags | Link |
|-------------|------|------|
|-------------|------|------|

|                                                                                            |                                                |                                                             |
|--------------------------------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------|
| JVN#93799513: WordPress plugin "Fudousan plugin" series vulnerable to cross-site scripting | <a href="#">jvn.jp</a><br>text/xml             | MISC<br><a href="#">jvn.jp/en/jp/JVN93799513/index.html</a> |
| 不動産プラグイン(本体)   WordPress 不動産プラグインで不動産ホームページ                                                | <a href="#">nendeb.jp</a><br>text/html         | MISC <a href="#">nendeb.jp/fudou</a>                        |
| 不動産プラグインシリーズ 6月のバージョンアップと脆弱性の対応を行いました   不動産プラグインマーケット                                      | <a href="#">www.nendeb-biz.jp</a><br>text/html | MISC <a href="#">www.nendeb-biz.jp/2021-0617-1200/</a>      |

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="#">Nendeb</a> | <a href="#">Fudousan Plugin</a>                 | All     | All    | All     | All      |
| Application                                                 | <a href="#">Nendeb</a> | <a href="#">Fudousan Plugin Pro Multi-user</a>  | All     | All    | All     | All      |
| Application                                                 | <a href="#">Nendeb</a> | <a href="#">Fudousan Plugin Pro Single-user</a> | All     | All    | All     | All      |
| cpe:2.3:a:nendeb:fudousan_plugin:*:*:*:*:*:                 |                        |                                                 |         |        |         |          |
| cpe:2.3:a:nendeb:fudousan_plugin_pro_multi-user:*:*:*:*:*:  |                        |                                                 |         |        |         |          |
| cpe:2.3:a:nendeb:fudousan_plugin_pro_single-user:*:*:*:*:*: |                        |                                                 |         |        |         |          |

No vendor comments have been submitted for this CVE

Social Mentions

| Source     | Title                                                                                                                                                                | Posted (UTC)        |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| @CVEreport | CVE-2021-20749 : Cross-site scripting vulnerability in Fudousan plugin ver5.7.0 and earlier, Fudousan Plugin Pro Si... <a href="#">twitter.com/i/web/status/1...</a> | 2021-06-28 00:56:03 |
| /r/netcve  | <a href="#">CVE-2021-20749</a>                                                                                                                                       | 2021-06-28 01:41:40 |

[← Previous ID](#)

[Next ID →](#)