



# CVE-2021-4134

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-4134
<b>State</b>	PUBLIC
<b>Assigner</b>	security@wordfence.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-02-16 17:15:00 UTC
<b>Updated</b>	2022-02-24 03:25:00 UTC
<b>Description</b>	The Fancy Product Designer WordPress plugin is vulnerable to SQL Injection due to insufficient escaping and parameteriza

## Risk And Classification

**Problem Types:** CWE-89

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Radykal	Fancy Product Designer	All	All	All	All

## References

Reference	Source	Link	Tags
4.7.5 : Fancy Product Designer	MISC	<a href="https://support.fancyproductdesigner.com">support.fancyproductdesigner.com</a>	Release Notes, Vendor Advisory
Vulnerability Advisories - Wordfence	MISC	<a href="https://www.wordfence.com">www.wordfence.com</a>	Exploit, Third Party Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Lin Yu

There are currently no legacy QID mappings associated with this CVE.

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)