Fancy Product Designer <= 4.6.9 - Insufficient Authorization to Arbitrary Options Update via fpd_update_options

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-4334
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-20 08:15:11 UTC
Updated	2026-04-08 19:17:40 UTC
Description	The Fancy Product Designer plugin for WordPress is vulnerable to unauthorized modification of site options due to a missin

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.001140000 probability, percentile 0.300730000 (date 2026-04-09)

Problem Types: CWE-285 | CWE-863 | CWE-285 CWE-285 Improper Authorization

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	security@wordfence.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Radykal	Fancy Product Designer	affected 4.6.9 semver	Not specified

References

Reference	Source
Fancy Product Designer <= 4.6.9 - Insufficient Authorization to Arbitrary Options Update via fpd_update_options	af854a3a-2127-422b-91ae
4.7.0 : Fancy Product Designer	af854a3a-2127-422b-91ae
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Ramuel Gall (en)

Additional Advisory Data

Source	Time	Event
CNA	2021-06-09T00:00:00.000Z	Vendor Notified
CNA	2023-04-05T00:00:00.000Z	Disclosed

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

Free CVE JSON API cve.report/api

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