



# WordPress FastDup Plugin <= 2.1.7 is vulnerable to Sensitive Data Exposure

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

## Summary

<b>CVE</b>	CVE-2023-51406
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-01-08 21:15:08 UTC
<b>Updated</b>	2026-04-28 19:22:43 UTC
<b>Description</b>	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ninja Team FastDup – Fastest WordPress Migr

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from nvd@nist.gov

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

**EPSS:** 0.006930000 probability, percentile 0.719140000 (date 2026-04-28)

**Problem Types:** CWE-200 | NVD-CWE-noinfo | CWE-200 CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	audit@patchstack.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Ninjateam</a>	<a href="#">Fastdup</a>	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Ninja Team</a>	<a href="#">FastDup Fastest WordPress Migration Duplicator</a>	affected n/a 2.1.7 custom	Not specified

#### References

Reference	Source	Link
<a href="#">patchstack.com/database/vulnerability/fastdup/wordpress-fastdup-plugin-2-1-7...</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="#">patchstack.co</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Joshua Chan (Patchstack Alliance) (en)

#### Additional Advisory Data

Solutions

**CNA:** Update to 2.1.8 or a higher version.

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

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)