WordPress Export Users Data Distinct Plugin <= 1.3 is vulnerable to CSV Injection

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

Summary

CVE	CVE-2022-46804
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-07 17:15:08 UTC
Updated	2026-04-28 19:19:06 UTC
Description	Improper Neutralization of Formula Elements in a CSV File vulnerability in Narola Infotech Solutions LLP Export Users Data

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

Problem Types: CWE-1236 | CWE-1236 CWE-1236 Improper Neutralization of Formula Elements in a CSV File

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	audit@patchstack.com	Secondary	5.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:N/I:H/A:N
3.1	CNA	CVSS	5.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

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	Narolainfotech	Export Users Data Distinct	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Narola Infotech Solutions LLP	Export Users Data Distinct	affected n/a 1.3 custom	Not specified

References

Reference	Source	Link
WordPress Export Users Data Distinct plugin <= 1.3 - CSV Injection - Patchstack	af854a3a-2127-422b-91ae-364da2661108	patchstack.c
patchstack.com/database/Wordpress/Plugin/export-users-data-distinct/vulnerab...	MITRE	patchstack.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Mika (Patchstack Alliance) (en)

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

© CVE.report 2026 |
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 registred 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

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