



WordPress Export Users Data CSV Plugin <= 2.1 is vulnerable to CSV Injection

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2022-41616
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-07 18:15:07 UTC
Updated	2026-04-28 19:18:48 UTC
Description	Improper Neutralization of Formula Elements in a CSV File vulnerability in Kaushik Kalathiya Export Users Data CSV. This i

Risk And Classification

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

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/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:N/UI:R/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	audit@patchstack.com	Secondary	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kaushikkalathiya	Export Users Data	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Kaushik Kalathiya	Export Users Data CSV	affected n/a 2.1 custom	Not specified

References

Reference	Source
WordPress Export Users Data CSV plugin <= 2.1 - Auth. CSV Injection vulnerability - Patchstack	af854a3a-2127-422b-91ae-364da2661106
patchstack.com/database/Wordpress/Plugin/export-users-data-csv/vulnerability...	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: [Mika \(Patchstack Alliance\)](#) (en)

Additional Advisory Data

Solutions

CNA: Update to 2.2 or a higher version.

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

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

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