



WordPress WP CSV Exporter Plugin <= 2.0 is vulnerable to CSV Injection

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2022-38702
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 19:18:43 UTC
Description	Improper Neutralization of Formula Elements in a CSV File vulnerability in Nakashima Masahiro WP CSV Exporter.This iss

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	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	None
User Interaction	Required
Scope	Unchanged
Confidentiality	High

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	Kigurumi	Csv Exporter	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Nakashima Masahiro	WP CSV Exporter	affected n/a 2.0 custom	Not specified

References

Reference	Source	Link
WordPress WP CSV Exporter plugin <= 2.0 - Auth. CSV Injection Vulnerability - Patchstack	af854a3a-2127-422b-91ae-364da2661108	patchstack.com/database/Wordpress/Plugin/wp-csv-exporter/vulnerability/wordp...
patchstack.com/database/Wordpress/Plugin/wp-csv-exporter/vulnerability/wordp...	MITRE	
CVE Program record	CVE.ORG	
NVD vulnerability detail	NVD	

Vendor Comments And Credit

Discovery Credit

CNA: Mika (Patchstack Alliance) (en)

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