EditorsKit <= 1.40.3 - Authenticated (Administrator+) Arbitrary File Upload

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

Summary

CVE	CVE-2023-6635
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-02-05 22:15:56 UTC
Updated	2026-04-08 18:18:39 UTC
Description	The EditorsKit plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation on the 'import_s

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from nvd@nist.gov

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

Problem Types: CWE-434 | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	security@wordfence.com	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/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	Extendify	Editorskit	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Munirkamal	Gutenberg Block Editor Toolkit EditorsKit	affected 1.40.3 semver	Not specified

References

Reference	Source	L
plugins.trac.wordpress.org/changeset/3010794/block-options	af854a3a-2127-422b-91ae-364da2661108	p
www.wordfence.com/threat-intel/vulnerabilities/id/4528f9a1-7027-4aa9-b006-bea84...	af854a3a-2127-422b-91ae-364da2661108	w
plugins.trac.wordpress.org/browser/block-options/tags/1.40.3/includes/addons/styles-mana...	af854a3a-2127-422b-91ae-364da2661108	p
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

Vendor Comments And Credit

Discovery Credit

CNA: István Márton (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-12-08T00:00:00.000Z	Discovered
CNA	2023-12-08T00:00:00.000Z	Vendor Notified
CNA	2023-12-16T00:00:00.000Z	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