Events Made Easy <= 2.3.16 - Missing Authorization

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

Summary

CVE	CVE-2023-0404
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-19 15:15:14 UTC
Updated	2026-04-08 18:17:42 UTC
Description	The Events Made Easy plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on sev

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	security@wordfence.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	E-dynamics	Events Made Easy	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Liedekef	Events Made Easy	affected 2.3.16 semver	Not specified

References

Reference	Source	Link
Events Made Easy <= 2.3.16 - Missing Authorization	af854a3a-2127-422b-91ae-364da2661108	www.wor
www.wordfence.com/threat-intel/vulnerabilities/id/5a9e62de-3e70-424f-b8e5-2a5f0...	security@wordfence.com	www.wor
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	plugins.tr
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: Marco Wotschka (en)

Additional Advisory Data

Source	Time	Event
CNA	2022-12-23T00:00:00.000Z	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**