



Easy Custom Auto Excerpt <= 2.4.12 - Sensitive Information Exposure

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2024-3312
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-02 17:15:24 UTC
Updated	2026-04-08 18:21:23 UTC
Description	The Easy Custom Auto Excerpt plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including 2.4.12. An attacker with knowledge of the vulnerability and access to the WordPress site can retrieve sensitive information from the database.

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from security@wordfence.com

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

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

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None

Availability

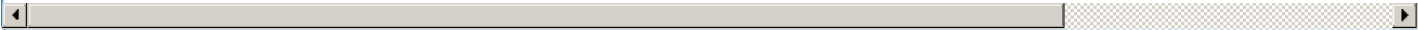
None

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



Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Todiadiatmo	Easy Custom Auto Excerpt	affected 2.4.12 semver	Not specified
ADP	Tonjoostudio	Easy Custom Auto Excerpt	affected 2.4.12 custom	Not specified

References		
Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/8c1e1fe4-23be-4f66-ae9f-cabb8...	af854a3a-2127-422b-91ae-364da2661108	www.worc
plugins.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	plugins.tr
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.g



Vendor Comments And Credit	
Discovery Credit	
CNA: Krzysztof Zajac (en)	

Additional Advisory Data		
Source	Time	Event
CNA	2024-04-18T00:00:00.000Z	Disclosed

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