ImageRecycle pdf & image compression <= 3.1.13 - Missing Authorization to Settings Update in enableOptimization

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

Summary

CVE	CVE-2024-0983
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-02-29 01:43:34 UTC
Updated	2026-04-08 17:17:27 UTC
Description	The ImageRecycle pdf & image compression plugin for WordPress is vulnerable to unauthorized modification of data due to

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from security@wordfence.com

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

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

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
None

ntegrity

Low

vailability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagerecycle	Imagerecycle Pdf Image Compression	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Imagerecycle	ImageRecycle Pdf Image Compression	affected 3.1.13 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset/3031424/imagerecycle-pdf-image-compression	af854a3a-2127-422b-91ae-364da2661108	plugins.t
www.wordfence.com/threat-intel/vulnerabilities/id/175dd04d-ce06-45a0-8cfe-14498...	af854a3a-2127-422b-91ae-364da2661108	www.wo
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

Vendor Comments And Credit

Discovery Credit

CNA: Francesco Carlucci (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-01-30T00:00:00.000Z	Vendor Notified
CNA	2024-02-07T00:00:00.000Z	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**