eMagicOne Store Manager for WooCommerce <= 1.2.5 - Unauthenticated Arbitrary File Upload via set_file()

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

Summary

CVE	CVE-2025-4336
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-05-24 04:15:27 UTC
Updated	2026-04-08 18:24:47 UTC
Description	The eMagicOne Store Manager for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missi

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/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	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	security@wordfence.com	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/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	Emagicone	Emagicone Store Manager For Woocommerce	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Emagicone	EMagicOne Store Manager For WooCommerce	affected 1.2.5 semver	Not specified

References

Reference	Source	Link
github.com/d0n601/CVE-2025-4336	security@wordfence.com	github.com
ryankozak.com/posts/cve-2025-4336	security@wordfence.com	ryankozak.com
plugins.trac.wordpress.org/browser/store-manager-connector/trunk/classes/class-emosmcwoo...	security@wordfence.com	plugins.trac.wo
plugins.trac.wordpress.org/browser/store-manager-connector/trunk/classes/class-emosmcwoo...	security@wordfence.com	plugins.trac.wo
plugins.trac.wordpress.org/changeset/3308544	security@wordfence.com	plugins.trac.wo
www.wordfence.com/threat-intel/vulnerabilities/id/5323dbb7-3893-4b43-838b-63265...	security@wordfence.com	www.wordfenc
plugins.trac.wordpress.org/browser/store-manager-connector/trunk/smconnector.php	security@wordfence.com	plugins.trac.wo
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Ryan Kozak (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-05-23T14:33:08.000Z	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