Easy WP SMTP by SendLayer <= 2.3.0 - Exposure of Sensitive Information via the UI

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

Summary

CVE	CVE-2024-3073
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-06-13 09:15:13 UTC
Updated	2026-04-08 19:21:15 UTC
Description	The Easy WP SMTP by SendLayer – WordPress SMTP and Email Log Plugin plugin for WordPress is vulnerable to informa

Risk And Classification

Primary CVSS: v3.1 2.7 LOW from security@wordfence.com

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

EPSS: 0.002530000 probability, percentile 0.486550000 (date 2026-04-13)

Problem Types: CWE-257 | NVD-CWE-noinfo | CWE-257 CWE-257 Storing Passwords in a Recoverable Format

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	2.7	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	2.7	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wp-ecommerce	Easy Wp Smtp	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Smub	Easy WP SMTP WordPress SMTP And Email Logs Gmail Office 365 Outlook Custom SMTP And More	affected 2.3.0 s

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/b043197c-4477-4663-abb8-58401...	af854a3a-2127-422b-91ae-364da2661108	www.wo
plugins.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	plugins.
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Discovery Credit

CNA: Andy Gilbert (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-06-12T20:02:54.000Z	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**