WP Encryption – One Click Free SSL Certificate & SSL / HTTPS Redirect to Force HTTPS, SSL Score <= 7.0 - Sensitive Information Exposure via insufficiently protected files

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

Summary

CVE	CVE-2023-7046
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-09 19:15:13 UTC
Updated	2026-04-08 18:18:47 UTC
Description	The WP Encryption – One Click Free SSL Certificate & SSL / HTTPS Redirect to Force HTTPS, SSL Score plugin for Word

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security@wordfence.com

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

Problem Types: CWE-200 | CWE-200 CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	F
CNA	Gowebsmarty	WP Encryption One Click Free SSL Certificate SSL / HTTPS Redirect Security SSL Scan	affected 7.0 semver	N
ADP	Gowebsmarty	Wp-encryption	affected 7.0 semver	N

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/7ab99751-24b7-41db-8a27-d86ed...	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: Krzysztof Zając (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-04-09T00:00:00.000Z	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**