



Email Encoder < 2.3.4 - Admin+ Stored XSS

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2024-7083
State	PUBLISHED
Assigner	WPScan
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-20 07:16:14 UTC
Updated	2026-04-20 07:16:14 UTC
Description	The Email Encoder WordPress plugin before 2.3.4 does not sanitise and escape some of its settings, which could allow hig

Risk And Classification

Problem Types: CWE-79 Cross-Site Scripting (XSS)

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Unknown	Email Encoder	affected 2.3.4 semver	Not specified

References

Reference	Source	Link	Tags
wpscan.com/vulnerability/7aeb6891-e159-4ed8-b1a9-a551140c9fcc	contact@wpscan.com	wpscan.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Dmitrii Ignatyev (en)

CNA: WPScan (en)

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)