



CVE-2021-24257

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

Summary

CVE	CVE-2021-24257
State	PUBLIC
Assigner	contact@wpscan.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-05 19:15:00 UTC
Updated	2021-05-11 15:03:00 UTC
Description	The "Premium Addons for Elementor" WordPress Plugin before 4.2.8 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) attacks. An attacker can inject malicious JavaScript code into the widget's output, which is then executed in the browser of the user. This can lead to various attacks, including session hijacking, data theft, and defacement of the website.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Leap13	Premium Addons For Elementor	All	All	All	All

References

Reference	Source	Link	Tags
Attention Required! Cloudflare	CONFIRM	wpscan.com	
Recent Patches Rock the Elementor Ecosystem	MISC	www.wordfence.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

LEGACY: Ramuel Gall

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