



# CVE-2023-32243

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

## Summary

<b>CVE</b>	CVE-2023-32243
<b>State</b>	PUBLIC
<b>Assigner</b>	audit@patchstack.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-12 08:15:00 UTC
<b>Updated</b>	2023-05-23 20:17:00 UTC
<b>Description</b>	Improper Authentication vulnerability in WPDeveloper Essential Addons for Elementor allows Privilege Escalation. This issue

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wpdeveloper	Essential Addons For Elementor	All	All	All	All

## References

Reference	Source
WordPress Elementor Lite 5.7.1 Arbitrary Password Reset ~ Packet Storm	MISC
Critical Privilege Escalation in Essential Addons for Elementor Plugin Affecting 1+ Million Sites	MISC
WordPress Essential Addons for Elementor plugin 5.4.0-5.7.1 - Unauthenticated Privilege Escalation vulnerability - Patchstack	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[150686](#) WordPress Essential Addons for Elementor Plugin: Improper Authentication Vulnerability (CVE-2023-32243)

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](#)