



# CVE-2022-29455

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

## Summary

<b>CVE</b>	CVE-2022-29455
<b>State</b>	PUBLIC
<b>Assigner</b>	audit@patchstack.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-06-13 17:15:00 UTC
<b>Updated</b>	2022-06-27 16:18:00 UTC
<b>Description</b>	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 ve

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elementor	Website Builder	All	All	All	All

## References

Reference	Source
Elementor Website Builder – WordPress plugin   WordPress.org	CONFID
WordPress Elementor plugin <= 3.5.5 - Unauthenticated DOM-based Reflected Cross-Site Scripting (XSS) vulnerability - Patchstack	CONFID
Hacking 6.5+ million websites => CVE-2022-29455 (Elementor)	CONFID
CVE Program record	CVE.O
NVD vulnerability detail	NVD

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Vulnerability discovered by Rotem Bar (Patchstack Alliance)

## Legacy QID Mappings

150529 WordPress Elementor Plugin: DOM-based Reflected Cross-Site Scripting (XSS) Vulnerability (CVE-2022-29455)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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