



WordPress Draft Plugin <= 3.0.9 - Cross Site Scripting (XSS) Vulnerability

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

Summary

CVE CVE-2025-58033

State PUBLISHED

Assigner Patchstack

Source Priority CVE Program / NVD first with legacy fallback

Published 2025-09-22 19:16:06 UTC

Updated 2026-04-01 17:26:56 UTC

Description Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in leeshadle Draft website

Risk And Classification

EPSS: 0.000330000 probability, percentile 0.096590000 (date 2026-04-02)

Problem Types: CWE-79 | CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Leeshadle	Draft	affected 3.0.9 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/website-builder/vulnerability/wordp...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

Vendor Comments And Credit

Discovery Credit

CNA: Nabil Irawan | Patchstack Bug Bounty Program (en)

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

© [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](#)