WordPress Plugin Vulnerabilities

Newsletter < 8.7.1 - Admin+ Stored XSS

Description

The plugin does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).

Proof of Concept

```
Put the following payload in the 'Custom styles' Advanced settings of the plugin (/w

The XSS will be triggered in any frontend form generated by the plugin
```

Affects Plugins

newsletter

Fixed in 8.7.1 ✓

References

CVE

CVE-2025-3583

URL

https://research.cleantalk.org/cve-2025-3583/

Classification

Type
XSS

OWASP top 10
A7: Cross-Site Scripting (XSS)

CWE
CWE-79

CVSS
3.5 (low)

Miscellaneous

Original Researcher
Dmitrii Ignatyev

Submitter
Dmitrii Ignatyev

Submitter website
https://www.linkedin.com/in/dmitriy-ignatyev-8a9189267/

Verified
Yes

WPVDB ID
a6582e14-e21e-48e7-9b4c-0044fb199825

Timeline

Publicly Published
2025-04-14 (about 21 days ago)

Added

2025-04-14 (about 21 days ago)

Last Updated

2025-04-14 (about 21 days ago)

Other

Published
2025-01-07
Title
StorePress <= 1.0.12 - Authenticated (Contributor+) Stored Cross-Site Scripting

Published
2020-01-22
Title
Contact Form Clean and Simple < 4.7.1 - Authenticated Stored XSS

Published
2024-05-21
Title
Element Pack Elementor Addons < 5.6.2 - Contributor+ Stored XSS

Published
2024-10-21
Title
LaTeX2HTML < 2.5.5 - Reflected Cross-Site Scripting

Published
2021-09-08
Title
3D Cover Carousel <= 1.0 - Reflected Cross-Site Scripting