WordPress Plugin Vulnerabilities

SureForms < 1.4.4 - Admin+ Stored XSS

Description

The plugin does not sanitise and escape some of its Form 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

```
1) Create a new Blank Form
2) Put an Email block
3) Go to "Form Confirmation" settings, put the following payload in the "Confirmatio
3) The XSS will be triggered when a user will submit data to the form
```

Affects Plugins

sureforms

Fixed in 1.4.4 ✓

References

CVE

CVE-2025-3513

URL

https://research.cleantalk.org/cve-2025-3513/

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
dd7e0bb3-4a98-4f62-bd2e-f30b27d71226

Timeline

Publicly Published

2025-04-11 (about 22 days ago)

Added

2025-04-11 (about 22 days ago)

Last Updated

2025-04-11 (about 22 days ago)

Other

Published
2015-12-09
Title
WP Easy Poll <= 1.1.3 - Cross-Site Scripting (XSS) & CSRF

Published
2023-06-03
Title
Don8 <= 0.4 - Admin+ Stored XSS

Published
2024-12-27
Title
List category posts < 0.90.3 - Author+ Stored XSS

Published
2021-12-14
Title
H5P CSS Editor <= 1.0 - Reflected Cross-Site Scripting

Published
2010-11-01
Title
Cforms <= 13.1 - 'lib_ajax.php' Cross-Site Scripting (XSS)