



CVE-2014-4605

Published on: 07/02/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:44 PM UTC

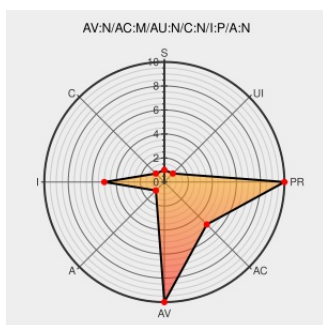
CVE-2014-4605

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Zdstatistics](#) from [Zdstatistics Project](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in cal/test.php in the ZdStatistics (zdstats) plugin 2.0.1 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the lang parameter.

CVE-2014-4605 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

wp-plugin : zdstats – A3-Cross-Site Scripting (XSS) | Code Vigilant

[Exploit](#)
[codevigilant.com](#)
[text/html](#)

[MISC codevigilant.com/disclosure/wp-plugin-zdstats-a3-cross-site-scripting-xss](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zdstatistics Project	Zdstatistics	All	-	-	All
cpe:2.3:a:zdstatistics_project:zdstatistics:*:*:*:*:wordpress:*:*:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID →		