



CVE-2009-2851

Published on: 08/18/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:30 PM UTC

CVE-2009-2851

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Cross-site scripting (XSS) vulnerability in the administrator interface in WordPress before 2.8.2 allows remote attackers to inject arbitrary web script or HTML via a comment author URL.

CVE-2009-2851 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

[SECURITY] Fedora 11 Update: wordpress-2.8.2-1.fc11

[Mailing List](#)
[Third Party Advisory](#)
[www.redhat.com](#)
[text/html](#)

[FEDORA FEDORA-2009-8109](#)

Debian -- Security Information -- DSA-1871-1 wordpress

[Third Party Advisory](#)
[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-1871](#)

oss-security - CVE Request -- WordPress

[Mailing List](#)
[Third Party Advisory](#)
[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20090721 CVE Request -- WordPress](#)

512900 -- (CVE-2009-2851) CVE-2009-2851 WordPress: XSS via unescaped HTML UURI s as author comments in the admin page

[Issue Tracking](#)
[Third Party Advisory](#)

[CONFIRM](#)
[bugzilla.redhat.com/show_bug.cgi?id=512900](#)

Unescaped HTML causes admin comments in the admin page	Third Party Advisory bugzilla.redhat.com text/html	bugzilla.redhat.com/show_bug.cgi?id=912000
SecurityTracker.com Archives - WordPress Input Validation Flaw in Comment Author URLs Permits Cross-Site Scripting Attacks	Third Party Advisory VDB Entry securitytracker.com text/html	 SECTrack 1022589
[SECURITY] Fedora 10 Update: wordpress-2.8.2-1.fc10	Mailing List Third Party Advisory www.redhat.com text/html	 FEDORA FEDORA-2009-8114
278492 –	Issue Tracking Third Party Advisory bugs.gentoo.org text/html	 CONFIRM bugs.gentoo.org/show_bug.cgi?id=278492
News – WordPress 2.8.2 – WordPress.org	Patch Vendor Advisory wordpress.org text/html	 CONFIRM wordpress.org/development/2009/07/wordpress-2-8-2/

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	Wordpress	Wordpress	All	All	All	All
cpe:2.3:a:wordpress:wordpress:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)