



CVE-2014-5240

Published on: 08/18/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:53 PM UTC

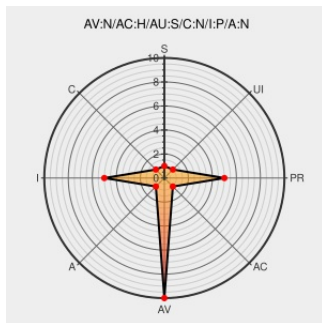
CVE-2014-5240

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Cross-site scripting (XSS) vulnerability in wp-includes/pluggable.php in WordPress before 3.9.2, when Multisite is enabled, allows remote authenticated administrators to inject arbitrary web script or HTML, and obtain Super Admin privileges, via a crafted avatar URL.

CVE-2014-5240 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access
Vector

NETWORK

Access
Complexity

HIGH

Authentication

SINGLE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Changeset 29398 – WordPress Trac

[web.archive.org](#)

[text/html](#)

Inactive Link Not Archived

[CONFIRM core.trac.wordpress.org/changeset/29398](#)

WordPress › WordPress 3.9.2 Security Release

[Patch](#)

[Vendor Advisory](#)

[wordpress.org](#)

[text/html](#)

[CONFIRM wordpress.org/news/2014/08/wordpress-3-9-2/](#)

Debian -- Security Information -- DSA-3001-1
wordpress

[www.debian.org](#)

Deprecated Link

[text/html](#)

[DEBIAN DSA-3001](#)

oss-security - Re: WordPress 3.9.2 release -
needs CVE's

[openwall.com](#)

[text/html](#)

[MLIST \[oss-security\] 20140813 Re: WordPress 3.9.2 release - needs CVE's](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

By selecting these links, you may be leaving CVEreport website. We have provided these links to external resources 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
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Wordpress	Wordpress	3.0	All	All	All
Application	Wordpress	Wordpress	3.0.1	All	All	All
Application	Wordpress	Wordpress	3.0.2	All	All	All
Application	Wordpress	Wordpress	3.0.3	All	All	All
Application	Wordpress	Wordpress	3.0.4	All	All	All
Application	Wordpress	Wordpress	3.0.5	All	All	All
Application	Wordpress	Wordpress	3.0.6	All	All	All
Application	Wordpress	Wordpress	3.1	All	All	All
Application	Wordpress	Wordpress	3.1.1	All	All	All
Application	Wordpress	Wordpress	3.1.2	All	All	All
Application	Wordpress	Wordpress	3.1.3	All	All	All
Application	Wordpress	Wordpress	3.1.4	All	All	All
Application	Wordpress	Wordpress	3.2	All	All	All
Application	Wordpress	Wordpress	3.2	beta1	All	All
Application	Wordpress	Wordpress	3.2.1	All	All	All
Application	Wordpress	Wordpress	3.3	All	All	All
Application	Wordpress	Wordpress	3.3.1	All	All	All
Application	Wordpress	Wordpress	3.3.2	All	All	All
Application	Wordpress	Wordpress	3.3.3	All	All	All
Application	Wordpress	Wordpress	3.4.0	All	All	All
Application	Wordpress	Wordpress	3.4.1	All	All	All
Application	Wordpress	Wordpress	3.4.2	All	All	All
Application	Wordpress	Wordpress	3.5.0	All	All	All
Application	Wordpress	Wordpress	3.5.1	All	All	All
Application	Wordpress	Wordpress	3.6	All	All	All

Application	Wordpress	Wordpress	3.6.1	All	All	All
Application	Wordpress	Wordpress	3.7	All	All	All
Application	Wordpress	Wordpress	3.7.1	All	All	All
Application	Wordpress	Wordpress	3.8	All	All	All
Application	Wordpress	Wordpress	3.8.1	All	All	All
Application	Wordpress	Wordpress	3.9.0	All	All	All
Application	Wordpress	Wordpress	3.0	All	All	All
Application	Wordpress	Wordpress	3.0.1	All	All	All
Application	Wordpress	Wordpress	3.0.2	All	All	All
Application	Wordpress	Wordpress	3.0.3	All	All	All
Application	Wordpress	Wordpress	3.0.4	All	All	All
Application	Wordpress	Wordpress	3.0.5	All	All	All
Application	Wordpress	Wordpress	3.0.6	All	All	All
Application	Wordpress	Wordpress	3.1	All	All	All
Application	Wordpress	Wordpress	3.1.1	All	All	All
Application	Wordpress	Wordpress	3.1.2	All	All	All
Application	Wordpress	Wordpress	3.1.3	All	All	All
Application	Wordpress	Wordpress	3.1.4	All	All	All
Application	Wordpress	Wordpress	3.2	All	All	All
Application	Wordpress	Wordpress	3.2	beta1	All	All
Application	Wordpress	Wordpress	3.2.1	All	All	All
Application	Wordpress	Wordpress	3.3	All	All	All
Application	Wordpress	Wordpress	3.3.1	All	All	All
Application	Wordpress	Wordpress	3.3.2	All	All	All
Application	Wordpress	Wordpress	3.3.3	All	All	All
Application	Wordpress	Wordpress	3.4.0	All	All	All
Application	Wordpress	Wordpress	3.4.1	All	All	All
Application	Wordpress	Wordpress	3.4.2	All	All	All
Application	Wordpress	Wordpress	3.5.0	All	All	All
Application	Wordpress	Wordpress	3.5.1	All	All	All
Application	Wordpress	Wordpress	3.6	All	All	All
Application	Wordpress	Wordpress	3.6.1	All	All	All
Application	Wordpress	Wordpress	3.7	All	All	All
Application	Wordpress	Wordpress	3.7.1	All	All	All
Application	Wordpress	Wordpress	3.8	All	All	All
Application	Wordpress	Wordpress	3.8.1	All	All	All

Application	wordpress	wordpress	3.8.1	All	All	All
Application	Wordpress	Wordpress	3.9.0	All	All	All
Application	Wordpress	Wordpress	All	All	All	All
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.0:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.0.1:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.0.2:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.0.3:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.0.4:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.0.5:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.0.6:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.1:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.1.1:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.1.2:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.1.3:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.1.4:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.2:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.2:beta1:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.2.1:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.3:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.3.1:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.3.2:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.3.3:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.4.0:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.4.1:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.4.2:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.5.0:*:*:*:*:*:						
cpe:2.3:a:wordpress:wordpress:3.5.1:*:*:*:*:*:						

cpe:2.3:a:wordpress:wordpress:3.6:****:*:
cpe:2.3:a:wordpress:wordpress:3.6.1:****:*:
cpe:2.3:a:wordpress:wordpress:3.7:****:*:
cpe:2.3:a:wordpress:wordpress:3.7.1:****:*:
cpe:2.3:a:wordpress:wordpress:3.8:****:*:
cpe:2.3:a:wordpress:wordpress:3.8.1:****:*:
cpe:2.3:a:wordpress:wordpress:3.9.0:****:*:
cpe:2.3:a:wordpress:wordpress:3.0:****:*:
cpe:2.3:a:wordpress:wordpress:3.0.1:****:*:
cpe:2.3:a:wordpress:wordpress:3.0.2:****:*:
cpe:2.3:a:wordpress:wordpress:3.0.3:****:*:
cpe:2.3:a:wordpress:wordpress:3.0.4:****:*:
cpe:2.3:a:wordpress:wordpress:3.0.5:****:*:
cpe:2.3:a:wordpress:wordpress:3.0.6:****:*:
cpe:2.3:a:wordpress:wordpress:3.1:****:*:
cpe:2.3:a:wordpress:wordpress:3.1.1:****:*:
cpe:2.3:a:wordpress:wordpress:3.1.2:****:*:
cpe:2.3:a:wordpress:wordpress:3.1.3:****:*:
cpe:2.3:a:wordpress:wordpress:3.1.4:****:*:
cpe:2.3:a:wordpress:wordpress:3.2:****:*:
cpe:2.3:a:wordpress:wordpress:3.2:beta1:****:*:
cpe:2.3:a:wordpress:wordpress:3.2.1:****:*:
cpe:2.3:a:wordpress:wordpress:3.3:****:*:
cpe:2.3:a:wordpress:wordpress:3.3.1:****:*:
cpe:2.3:a:wordpress:wordpress:3.3.2:****:*:
cpe:2.3:a:wordpress:wordpress:3.3.3:****:*:
cpe:2.3:a:wordpress:wordpress:3.4.0:****:*:
cpe:2.3:a:wordpress:wordpress:3.4.1:****:*:
cpe:2.3:a:wordpress:wordpress:3.4.2:****:*:

cpe:2.3:a:wordpress:wordpress:3.5.0:*****:
cpe:2.3:a:wordpress:wordpress:3.5.1:*****:
cpe:2.3:a:wordpress:wordpress:3.6:*****:
cpe:2.3:a:wordpress:wordpress:3.6.1:*****:
cpe:2.3:a:wordpress:wordpress:3.7:*****:
cpe:2.3:a:wordpress:wordpress:3.7.1:*****:
cpe:2.3:a:wordpress:wordpress:3.8:*****:
cpe:2.3:a:wordpress:wordpress:3.8.1:*****:
cpe:2.3:a:wordpress:wordpress:3.9.0:*****:
cpe:2.3:a:wordpress:wordpress:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)