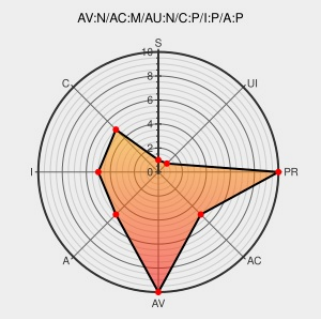
CVE-2013-2700

Published on: 05/14/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:42 PM UTC

CVE-2013-2700

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wp125 from Webmaster-source contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in the Add/Edit page (adminmenus.php) in the WP125 plugin before 1.5.0 for WordPress allows remote attackers to hijack the authentication of administrators for requests that add or edit an ad via unspecified vectors.

CVE-2013-2700 has been assigned by PSIRT-CNA@flexerasoftware.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
WordPress › WP125 « WordPress Plugins	wordpress.org, text/html	CONFIRM wordpress.org/plugins/wp125/changelog
About Secunia Research | Flexera	Vendor Advisory, secunia.com, Depreciated Link, text/plain	SECUNIA 52876
No Description Provided	osvdb.org, Inactive Link, Not Archived	OSVDB 92113
403 Forbidden	Exploit, Patch, plugins.trac.wordpress.org, text/html, Inactive Link, Not Archived	CONFIRM plugins.trac.wordpress.org/changeset/692721

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	Webmaster-source	Wp125	1.0.0	All	All	All
Application	Webmaster-source	Wp125	1.1.0	All	All	All
Application	Webmaster-source	Wp125	1.2.0	All	All	All
Application	Webmaster-source	Wp125	1.3.0	All	All	All
Application	Webmaster-source	Wp125	1.3.7	All	All	All
Application	Webmaster-source	Wp125	1.3.8	All	All	All
Application	Webmaster-source	Wp125	1.3.9	All	All	All
Application	Webmaster-source	Wp125	1.4.0	All	All	All
Application	Webmaster-source	Wp125	1.4.1	All	All	All
Application	Webmaster-source	Wp125	1.4.2	All	All	All
Application	Webmaster-source	Wp125	1.4.3	All	All	All
Application	Webmaster-source	Wp125	1.4.4	All	All	All
Application	Webmaster-source	Wp125	1.4.5	All	All	All
Application	Webmaster-source	Wp125	1.4.6	All	All	All
Application	Webmaster-source	Wp125	1.4.7	All	All	All
Application	Webmaster-source	Wp125	1.4.8	All	All	All
Application	Webmaster-source	Wp125	1.0.0	All	All	All
Application	Webmaster-source	Wp125	1.1.0	All	All	All
Application	Webmaster-source	Wp125	1.2.0	All	All	All
Application	Webmaster-source	Wp125	1.3.0	All	All	All
Application	Webmaster-source	Wp125	1.3.7	All	All	All
Application	Webmaster-source	Wp125	1.3.8	All	All	All
Application	Webmaster-source	Wp125	1.3.9	All	All	All
Application	Webmaster-source	Wp125	1.4.0	All	All	All
Application	Webmaster-source	Wp125	1.4.1	All	All	All
Application	Webmaster-source	Wp125	1.4.2	All	All	All
Application	Webmaster-source	Wp125	1.4.3	All	All	All

Application	Webmaster-source	Wp125	1.4.4	All	All	All
Application	Webmaster-source	Wp125	1.4.5	All	All	All
Application	Webmaster-source	Wp125	1.4.6	All	All	All
Application	Webmaster-source	Wp125	1.4.7	All	All	All
Application	Webmaster-source	Wp125	1.4.8	All	All	All
Application	Webmaster-source	Wp125	All	All	All	All

cpe:2.3:a:webmaster-source:wp125:1.0.0:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.1.0:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.2.0:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.3.0:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.3.7:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.3.8:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.3.9:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.0:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.1:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.2:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.3:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.4:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.5:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.6:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.7:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.8:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.0.0:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.1.0:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.2.0:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.3.0:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.3.7:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.3.8:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.3.9:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.0:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.1:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.2:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.3:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.4:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.5:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.6:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.7:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:1.4.8:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webmaster-source:wp125:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→