

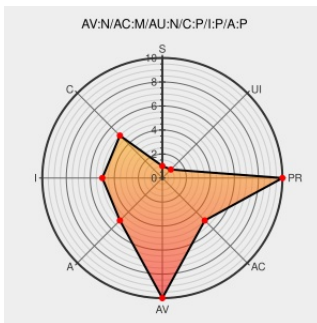


CVE-2006-1796

Published on: 04/17/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:59 PM UTC

CVE-2006-1796

[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 paging links functionality in template-functions-links.php in Wordpress 1.5.2, and possibly other versions before 2.0.1, allows remote attackers to inject arbitrary web script or HTML to Internet Explorer users via the request URI (`$_SERVER['REQUEST_URI']`).

CVE-2006-1796 has been assigned by [M](#) cve@mitre.org 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
#328909 - wordpress: CSS Security Vulnerability - Debian Bug report logs	Patch bugs.debian.org text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=328909
#1686 (CSS Security Vulnerability) - WordPress Trac - Trac	Patch web.archive.org text/html Inactive Link Not Archived	MISC trac.wordpress.org/ticket/1686

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	0.6.2	beta_2	All	All
Application	Wordpress	Wordpress	0.6.2.1	beta_2	All	All
Application	Wordpress	Wordpress	0.7	All	All	All
Application	Wordpress	Wordpress	0.71	All	All	All
Application	Wordpress	Wordpress	1.0	All	All	All
Application	Wordpress	Wordpress	1.0.1	All	All	All
Application	Wordpress	Wordpress	1.0.2	All	All	All
Application	Wordpress	Wordpress	1.2	All	All	All
Application	Wordpress	Wordpress	1.2.1	All	All	All
Application	Wordpress	Wordpress	1.2.2	All	All	All
Application	Wordpress	Wordpress	1.5	All	All	All
Application	Wordpress	Wordpress	1.5.1	All	All	All
Application	Wordpress	Wordpress	1.5.1.2	All	All	All
Application	Wordpress	Wordpress	1.5.1.3	All	All	All
Application	Wordpress	Wordpress	1.5.2	All	All	All
Application	Wordpress	Wordpress	2.0	All	All	All
Application	Wordpress	Wordpress	0.6.2	beta_2	All	All
Application	Wordpress	Wordpress	0.6.2.1	beta_2	All	All
Application	Wordpress	Wordpress	0.7	All	All	All
Application	Wordpress	Wordpress	0.71	All	All	All
Application	Wordpress	Wordpress	1.0	All	All	All
Application	Wordpress	Wordpress	1.0.1	All	All	All
Application	Wordpress	Wordpress	1.0.2	All	All	All
Application	Wordpress	Wordpress	1.2	All	All	All
Application	Wordpress	Wordpress	1.2.1	All	All	All
Application	Wordpress	Wordpress	1.2.2	All	All	All
Application	Wordpress	Wordpress	1.5	All	All	All
Application	Wordpress	Wordpress	1.5.1	All	All	All
Application	Wordpress	Wordpress	1.5.1.2	All	All	All
Application	Wordpress	Wordpress	1.5.1.3	All	All	All
Application	Wordpress	Wordpress	1.5.2	All	All	All

Application	Wordpress	Wordpress	All	All	All	All
	cpe:2.3:a:wordpress:wordpress:0.6.2:beta_2:*****:					
	cpe:2.3:a:wordpress:wordpress:0.6.2.1:beta_2:*****:					
	cpe:2.3:a:wordpress:wordpress:0.7:*****:					
	cpe:2.3:a:wordpress:wordpress:0.71:*****:					
	cpe:2.3:a:wordpress:wordpress:1.0:*****:					
	cpe:2.3:a:wordpress:wordpress:1.0.1:*****:					
	cpe:2.3:a:wordpress:wordpress:1.0.2:*****:					
	cpe:2.3:a:wordpress:wordpress:1.2:*****:					
	cpe:2.3:a:wordpress:wordpress:1.2.1:*****:					
	cpe:2.3:a:wordpress:wordpress:1.2.2:*****:					
	cpe:2.3:a:wordpress:wordpress:1.5:*****:					
	cpe:2.3:a:wordpress:wordpress:1.5.1:*****:					
	cpe:2.3:a:wordpress:wordpress:1.5.1.2:*****:					
	cpe:2.3:a:wordpress:wordpress:1.5.1.3:*****:					
	cpe:2.3:a:wordpress:wordpress:1.5.2:*****:					
	cpe:2.3:a:wordpress:wordpress:2.0:*****:					
	cpe:2.3:a:wordpress:wordpress:0.6.2:beta_2:*****:					
	cpe:2.3:a:wordpress:wordpress:0.6.2.1:beta_2:*****:					
	cpe:2.3:a:wordpress:wordpress:0.7:*****:					
	cpe:2.3:a:wordpress:wordpress:0.71:*****:					
	cpe:2.3:a:wordpress:wordpress:1.0:*****:					
	cpe:2.3:a:wordpress:wordpress:1.0.1:*****:					
	cpe:2.3:a:wordpress:wordpress:1.0.2:*****:					
	cpe:2.3:a:wordpress:wordpress:1.2:*****:					
	cpe:2.3:a:wordpress:wordpress:1.2.1:*****:					
	cpe:2.3:a:wordpress:wordpress:1.2.2:*****:					
	cpe:2.3:a:wordpress:wordpress:1.5:*****:					
	cpe:2.3:a:wordpress:wordpress:1.5.1:*****:					

cpe:2.3:a:wordpress:wordpress:1.5.1.2:*****:

cpe:2.3:a:wordpress:wordpress:1.5.1.3:*****:

cpe:2.3:a:wordpress:wordpress:1.5.2:*****:

cpe:2.3:a:wordpress:wordpress:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→