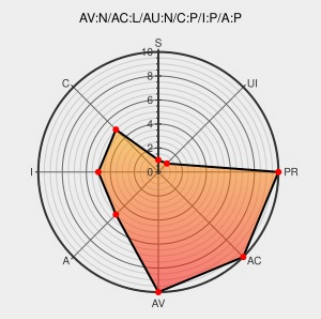
CVE-2007-4894

Published on: 09/14/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:33 PM UTC

CVE-2007-4894

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



Certain versions of Wordpress from Wordpress contain the following vulnerability:

Multiple SQL injection vulnerabilities in Wordpress before 2.2.3 and Wordpress multi-user (MU) before 1.2.5a allow remote attackers to execute arbitrary SQL commands via the post_type parameter to the pingback.extensions.getPingbacks method in the XMLRPC interface, and other unspecified parameters related to "early database escaping" and missing validation of "query string like parameters."

CVE-2007-4894 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Wordpress Script Insertion and SQL Injection Vulnerabilities - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 26771
Fedora update for wordpress - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 26796
#4770 (Fix mt_allow_pings in metaWeblog.newPost (XML-RPC)) - WordPress Trac - Trac	web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM trac.wordpress.org/ticket/4770
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com, text/html	VUPEN ADV-2007-3132

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF wordpress-wordpressmu-pingback-sql-injection(36578)
285831 – Upstream security fixes available	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=285831
Remote SQL Injection in Wordpress and Wordpress MU	www.buayacorp.com text/xml	MISC www.buayacorp.com/files/wordpress/wordpress-sql-injection-advisory.html
404 Not Found	fedoranews.org text/html Inactive Link Not Archived	FEDORA FEDORA-2007-2143
WordPress › Blog » WordPress 2.2.3	Patch wordpress.org text/html	CONFIRM wordpress.org/development/2007/09/wordpress-223/

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	All	All	All
Application	Wordpress	Wordpress	0.6.2.1	All	All	All
Application	Wordpress	Wordpress	0.7	All	All	All
Application	Wordpress	Wordpress	0.71	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	2.0	All	All	All
Application	Wordpress	Wordpress	2.0.1	All	All	All
Application	Wordpress	Wordpress	2.0.10_rc1	All	All	All
Application	Wordpress	Wordpress	2.0.10_rc2	All	All	All
Application	Wordpress	Wordpress	2.0.2	All	All	All
Application	Wordpress	Wordpress	2.0.3	All	All	All
Application	Wordpress	Wordpress	2.0.4	All	All	All

Application	Wordpress	Wordpress	2.0.5	All	All	All
Application	Wordpress	Wordpress	2.0.6	All	All	All
Application	Wordpress	Wordpress	2.0.7	All	All	All
Application	Wordpress	Wordpress	2.1.1	All	All	All
Application	Wordpress	Wordpress	2.1.2	All	All	All
Application	Wordpress	Wordpress	2.1.3	All	All	All
Application	Wordpress	Wordpress	2.1.3_rc1	All	All	All
Application	Wordpress	Wordpress	2.1.3_rc2	All	All	All
Application	Wordpress	Wordpress	2.2	All	All	All
Application	Wordpress	Wordpress	2.2.1	All	All	All
Application	Wordpress	Wordpress	2.2.2	All	All	All
Application	Wordpress	Wordpress	2.2_revision5002	All	All	All
Application	Wordpress	Wordpress	2.2_revision5003	All	All	All
Application	Wordpress	Wordpress	0.6.2	All	All	All
Application	Wordpress	Wordpress	0.6.2.1	All	All	All
Application	Wordpress	Wordpress	0.7	All	All	All
Application	Wordpress	Wordpress	0.71	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	2.0	All	All	All
Application	Wordpress	Wordpress	2.0.1	All	All	All
Application	Wordpress	Wordpress	2.0.10_rc1	All	All	All
Application	Wordpress	Wordpress	2.0.10_rc2	All	All	All
Application	Wordpress	Wordpress	2.0.2	All	All	All
Application	Wordpress	Wordpress	2.0.3	All	All	All
Application	Wordpress	Wordpress	2.0.4	All	All	All
Application	Wordpress	Wordpress	2.0.5	All	All	All
Application	Wordpress	Wordpress	2.0.6	All	All	All
Application	Wordpress	Wordpress	2.0.7	All	All	All
Application	Wordpress	Wordpress	2.1.1	All	All	All

Application	Wordpress	Wordpress	2.1.2	All	All	All
Application	Wordpress	Wordpress	2.1.3	All	All	All
Application	Wordpress	Wordpress	2.1.3_rc1	All	All	All
Application	Wordpress	Wordpress	2.1.3_rc2	All	All	All
Application	Wordpress	Wordpress	2.2	All	All	All
Application	Wordpress	Wordpress	2.2.1	All	All	All
Application	Wordpress	Wordpress	2.2.2	All	All	All
Application	Wordpress	Wordpress	2.2_revision5002	All	All	All
Application	Wordpress	Wordpress	2.2_revision5003	All	All	All

cpe:2.3:a:wordpress:wordpress:0.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:0.6.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:0.7:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:0.71:*:*:*:*:*:*:*:

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:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.10_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.10_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.1.3_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.1.3_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.2_revision5002:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.2_revision5003:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:0.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:0.6.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:0.7:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:0.71:*:*:*:*:*:*:*:

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:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.10_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.10_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.1.3_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.1.3_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.2_revision5002:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:2.2_revision5003:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→