



CVE-2008-4106

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2008-4106
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-09-18 17:59:00 UTC
Updated	2018-10-11 20:50:00 UTC
Description	WordPress before 2.6.2 does not properly handle MySQL warnings about insertion of username strings that exceed the ma

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wordpress	Wordpress	0.71-gold	All	All	All
Application	Wordpress	Wordpress	1.0-platinum	All	All	All
Application	Wordpress	Wordpress	1.0.1-miles	All	All	All
Application	Wordpress	Wordpress	1.0.2-blakey	All	All	All
Application	Wordpress	Wordpress	1.2-delta	All	All	All
Application	Wordpress	Wordpress	1.2-mingus	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-strayhorn	All	All	All
Application	Wordpress	Wordpress	1.5.1.1	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	2.0.1	All	All	All
Application	Wordpress	Wordpress	2.0.10	All	All	All
Application	Wordpress	Wordpress	2.0.11	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	2.0.9	All	All	All
Application	Wordpress	Wordpress	2.1	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	2.2	All	All	All
Application	Wordpress	Wordpress	2.2.1	All	All	All
Application	Wordpress	Wordpress	2.2.2	All	All	All
Application	Wordpress	Wordpress	2.2.3	All	All	All
Application	Wordpress	Wordpress	2.5	All	All	All
Application	Wordpress	Wordpress	2.5.1	All	All	All
Application	Wordpress	Wordpress	2.6	All	All	All
Application	Wordpress	Wordpress	0.71-gold	All	All	All
Application	Wordpress	Wordpress	1.0-platinum	All	All	All
Application	Wordpress	Wordpress	1.0.1-miles	All	All	All
Application	Wordpress	Wordpress	1.0.2-blakey	All	All	All
Application	Wordpress	Wordpress	1.2-delta	All	All	All
Application	Wordpress	Wordpress	1.2-mingus	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-strayhorn	All	All	All
Application	Wordpress	Wordpress	1.5.1.1	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	2.0.1	All	All	All
Application	Wordpress	Wordpress	2.0.10	All	All	All
Application	Wordpress	Wordpress	2.0.11	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	2.0.9	All	All	All
Application	Wordpress	Wordpress	2.1	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	2.2	All	All	All
Application	Wordpress	Wordpress	2.2.1	All	All	All
Application	Wordpress	Wordpress	2.2.2	All	All	All
Application	Wordpress	Wordpress	2.2.3	All	All	All
Application	Wordpress	Wordpress	2.5	All	All	All
Application	Wordpress	Wordpress	2.5.1	All	All	All
Application	Wordpress	Wordpress	2.6	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

References

Reference

WordPress Insecure Password Generation Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com

SecurityReason - Wordpress user_login Column SQL Truncation Vulnerability

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

News – WordPress 2.6.2 – WordPress.org

'Re: [oss-security] CVE request: wordpress < 2.6.2' - MARC

Fedora update for wordpress - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Wordpress 2.6.1 SQL Column Truncation Vulnerability

[SECURITY] Fedora 8 Update: wordpress-2.6.2-1.fc8

WordPress Lost Password SQL Column Truncation Unauthorized Access Vulnerability

404 Not Found

oss-security - CVE request: wordpress < 2.6.2

SecurityFocus

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

Wordpress 2.6.1 (SQL Column Truncation) Admin Takeover Exploit

Suspekt... » Blog Archive » MySQL and SQL Column Truncation Vulnerabilities

[SECURITY] Fedora 9 Update: wordpress-2.6.2-1.fc9

SecurityTracker.com Archives - WordPress SQL Truncation and Password Generation Flaw Lets Remote Users Determine the Administrator's

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)