



# CVE-2008-0664

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

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2008-0664                                                                                                            |
| <b>State</b>           | PUBLIC                                                                                                                   |
| <b>Assigner</b>        | cve@mitre.org                                                                                                            |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                             |
| <b>Published</b>       | 2008-02-08 02:00:00 UTC                                                                                                  |
| <b>Updated</b>         | 2011-03-08 03:05:00 UTC                                                                                                  |
| <b>Description</b>     | The XML-RPC implementation (xmlrpc.php) in WordPress before 2.3.3, when registration is enabled, allows remote attackers |

## Risk And Classification

### Problem Types: CWE-264

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                    | Product                   | Version    | Update | Edition | Language |
|-------------|---------------------------|---------------------------|------------|--------|---------|----------|
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 0.7        | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 0.71       | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.2        | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.2.1      | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.2.2      | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.3.1      | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.5        | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.5.1      | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.5.1.2    | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.5.1.3    | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.5.2      | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0        | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.1      | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.10     | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.10_rc1 | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.10_rc2 | All    | All     | All      |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.11     | All    | All     | All      |

|             |                           |                           |                  |     |     |     |
|-------------|---------------------------|---------------------------|------------------|-----|-----|-----|
|             |                           |                           |                  |     |     |     |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.2            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.3            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.4            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.5            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.6            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.7            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.1              | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.1.1            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.1.2            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.1.3            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.1.3_rc1        | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.1.3_rc2        | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.2              | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.2.1            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.2.2            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.2.3            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.2_revision5002 | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.2_revision5003 | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.3              | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.3.1            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.3.2            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 0.7              | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 0.71             | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.2              | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.2.1            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.2.2            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.3.1            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.5              | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.5.1            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.5.1.2          | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.5.1.3          | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 1.5.2            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0              | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.1            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.10           | All | All | All |

|             |                           |                           |                  |     |     |     |
|-------------|---------------------------|---------------------------|------------------|-----|-----|-----|
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.10_rc1       | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.10_rc2       | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.11           | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.2            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.3            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.4            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.5            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.6            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.0.7            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.1              | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.1.1            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.1.2            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.1.3            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.1.3_rc1        | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.1.3_rc2        | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.2              | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.2.1            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.2.2            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.2.3            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.2_revision5002 | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.2_revision5003 | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.3              | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.3.1            | All | All | All |
| Application | <a href="#">Wordpress</a> | <a href="#">Wordpress</a> | 2.3.2            | All | All | All |

| References                                                                                                |  |  |  |          |                                         |  |
|-----------------------------------------------------------------------------------------------------------|--|--|--|----------|-----------------------------------------|--|
| Reference                                                                                                 |  |  |  | Source   | Link                                    |  |
| OOPS!                                                                                                     |  |  |  | MISC     | <a href="#">www.village-idiot.com</a>   |  |
| WordPress XML-RPC Post Edit Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com |  |  |  | SECUNIA  | <a href="#">secunia.com</a>             |  |
| WordPress 'xmlrpc.php' Post Edit Unauthorized Access Vulnerability                                        |  |  |  | BID      | <a href="#">www.securityfocus.com</a>   |  |
| Fedora update for wordpress - Secunia Advisories - Vulnerability Intelligence - Secunia.com               |  |  |  | SECUNIA  | <a href="#">secunia.com</a>             |  |
| Debian -- Security Information -- DSA-1601-1 wordpress                                                    |  |  |  | DEBIAN   | <a href="#">www.debian.org</a>          |  |
| Bug 431547 – CVE-2008-0664 wordpress: XML-RPC interface vulnerability                                     |  |  |  | CONFIRM  | <a href="#">bugzilla.redhat.com</a>     |  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                          |  |  |  | VUPEN    | <a href="#">www.vupen.com</a>           |  |
| [SECURITY] Fedora 7 Update: wordpress-2.3.3-0.fc7                                                         |  |  |  | FEDORA   | <a href="#">www.redhat.com</a>          |  |
| SecurityTracker.com Archives - WordPress XML-RPC Bug Lets Remote Users Edit Arbitrary Posts               |  |  |  | SECTrack | <a href="#">www.securitytracker.com</a> |  |

|                                                                                             |         |                                                     |
|---------------------------------------------------------------------------------------------|---------|-----------------------------------------------------|
| News – WordPress 2.3.3 – WordPress.org                                                      | CONFIRM | <a href="https://wordpress.org">wordpress.org</a>   |
| Debian update for wordpress - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | <a href="https://secunia.com">secunia.com</a>       |
| [SECURITY] Fedora 8 Update: wordpress-2.3.3-0.fc8                                           | FEDORA  | <a href="https://www.redhat.com">www.redhat.com</a> |
| CVE Program record                                                                          | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>       |
| NVD vulnerability detail                                                                    | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>     |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)