



CVE-2007-1897

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

Summary

CVE	CVE-2007-1897
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-09 20:19:00 UTC
Updated	2017-10-11 01:32:00 UTC
Description	SQL injection vulnerability in xmlrpc (xmlrpc.php) in WordPress 2.1.2, and probably earlier, allows remote authenticated users to execute arbitrary code via the 'method' parameter.

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wordpress	Wordpress	2.1	All	All	All
Application	Wordpress	Wordpress	2.1.1	All	All	All
Application	Wordpress	Wordpress	2.1	All	All	All
Application	Wordpress	Wordpress	2.1.1	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

References

Reference	Source	Link	Tags
Wordpress 2.1.2 (xmlrpc) Remote SQL Injection Exploit	EXPLOIT-DB	www.exploit-db.com	
WordPress XML-RPC SQL Injection and Security Bypass - Advisories - Secunia	SECUNIA	secunia.com	Patch, Vendor Advisory
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Vendor Advisory
Debian -- Security Information -- DSA-1285-1 wordpress	DEBIAN	www.debian.org	
#4091 (XMLRPC SQL Injection and Security Bypass) – WordPress Trac	CONFIRM	trac.wordpress.org	
» Wordpress 2.1.2 xmlrpc Security Issues » www.otsosecure.com	MISC	www.otsosecure.com	Exploit, Vendor Advisory
WordPress Post_ID Parameter SQL Injection Vulnerability	BID	www.securityfocus.com	Exploit, Vendor Advisory
Debian update for wordpress - Advisories - Secunia	SECUNIA	secunia.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report