



CVE-2010-4403

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

Summary

CVE	CVE-2010-4403
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-12-06 13:37:00 UTC
Updated	2018-10-10 20:08:00 UTC
Description	The Register Plus plugin 3.5.1 and earlier for WordPress allows remote attackers to obtain sensitive information via a direct

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Devbits	Register-plus	1.1	All	All	All
Application	Devbits	Register-plus	1.2	All	All	All
Application	Devbits	Register-plus	2.0	All	All	All
Application	Devbits	Register-plus	2.1	All	All	All
Application	Devbits	Register-plus	2.2	All	All	All
Application	Devbits	Register-plus	2.3	All	All	All
Application	Devbits	Register-plus	2.4	All	All	All
Application	Devbits	Register-plus	2.5	All	All	All
Application	Devbits	Register-plus	2.6	All	All	All
Application	Devbits	Register-plus	2.7	All	All	All
Application	Devbits	Register-plus	2.8	All	All	All
Application	Devbits	Register-plus	2.9	All	All	All
Application	Devbits	Register-plus	3.0	All	All	All
Application	Devbits	Register-plus	3.0.1	All	All	All
Application	Devbits	Register-plus	3.0.2	All	All	All
Application	Devbits	Register-plus	3.1	All	All	All
Application	Devbits	Register-plus	3.2	All	All	All

Application	Devbits	Register-plus	3.3	All	All	All
Application	Devbits	Register-plus	3.4	All	All	All
Application	Devbits	Register-plus	3.4.1	All	All	All
Application	Devbits	Register-plus	3.5	All	All	All
Application	Devbits	Register-plus	1.1	All	All	All
Application	Devbits	Register-plus	1.2	All	All	All
Application	Devbits	Register-plus	2.0	All	All	All
Application	Devbits	Register-plus	2.1	All	All	All
Application	Devbits	Register-plus	2.2	All	All	All
Application	Devbits	Register-plus	2.3	All	All	All
Application	Devbits	Register-plus	2.4	All	All	All
Application	Devbits	Register-plus	2.5	All	All	All
Application	Devbits	Register-plus	2.6	All	All	All
Application	Devbits	Register-plus	2.7	All	All	All
Application	Devbits	Register-plus	2.8	All	All	All
Application	Devbits	Register-plus	2.9	All	All	All
Application	Devbits	Register-plus	3.0	All	All	All
Application	Devbits	Register-plus	3.0.1	All	All	All
Application	Devbits	Register-plus	3.0.2	All	All	All
Application	Devbits	Register-plus	3.1	All	All	All
Application	Devbits	Register-plus	3.2	All	All	All
Application	Devbits	Register-plus	3.3	All	All	All
Application	Devbits	Register-plus	3.4	All	All	All
Application	Devbits	Register-plus	3.4.1	All	All	All
Application	Devbits	Register-plus	3.5	All	All	All
Application	Devbits	Register-plus	All	All	All	All
Application	Wordpress	Wordpress	All	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

References						
Reference				Source	Link	Tags
SecurityFocus				BUGTRAQ	www.securityfocus.com	
Уразливості в Register Plus для WordPress - Websecurity - Веб безпека				MISC	websecurity.com.ua	Exploit
Register Plus For WordPress Cross Site Scripting / Path Disclosure ≈ Packet Storm				MISC	packetstormsecurity.org	Exploit
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](https://mitre.org/licenses).

Free CVE JSON API cve.report/api

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