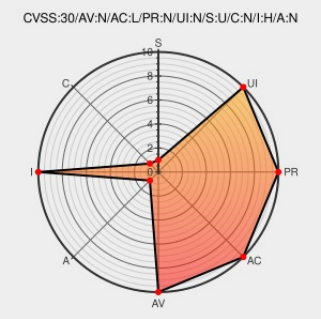
CVE-2017-1001000

Published on: 04/02/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:41 PM UTC

CVE-2017-1001000

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



Certain versions of Wordpress from Wordpress contain the following vulnerability:

The register_routes function in wp-includes/rest-api/endpoints/class-wp-rest-posts-controller.php in the REST API in WordPress 4.7.x before 4.7.2 does not require an integer identifier, which allows remote attackers to modify arbitrary pages via a request for wp-json/wp/v2/posts followed by a numeric value and a non-numeric value, as demonstrated by the wp-json/wp/v2/posts/123?id=123helloworld URI.

CVE-2017-1001000 has been assigned by josh@bress.net to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Content Injection Vulnerability in WordPress 4.7 and 4.7.1	Technical Description Third Party Advisory	MISC blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress-rest-

	blog.sucuri.net text/html	
Wordpress 4.7.0/4.7.1 Unauthenticated Content Injection PoC · GitHub	Issue Tracking Patch Third Party Advisory gist.github.com text/html	MISC gist.github.com/leonjza/2244eb15510a0687ed93160c623762ab
oss-security - Re: Asking for a CVE id for the WordPress Privilege Escalation vulnerability (4.7/4.7.1)	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20170210 Re: Asking for a CVE id for the WordPress P Escalation vulnerability (4.7/4.7.1)
WordPress Bugs Let Remote Users Conduct Cross-Site Scripting and SQL Injection Attacks, Obtain Potentially Sensitive Information, and Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1037731
WordPress 4.7.2 Security Release	Patch Release Notes Vendor Advisory wordpress.org text/html	CONFIRM wordpress.org/news/2017/01/wordpress-4-7-2-security-release/
REST API: Unify object access handling for simplicity. · WordPress/WordPress@e357195 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	CONFIRM github.com/WordPress/WordPress/commit/e357195ce303017d517aff944644a7
WordPress Web API Vulnerability - The Akamai Blog	Exploit Third Party Advisory blogs.akamai.com text/html	MISC blogs.akamai.com/2017/02/wordpress-web-api-vulnerability.html
Disclosure of Additional Security Fix in WordPress 4.7.2 – Make WordPress Core	Patch Vendor Advisory make.wordpress.org text/html	CONFIRM make.wordpress.org/core/2017/02/01/disclosure-of-additional-se wordpress-4-7-2/
Version 4.7.2 « WordPress Codex	Patch Vendor Advisory codex.wordpress.org text/html	CONFIRM codex.wordpress.org/Version_4.7.2

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	4.7	All	All	All

Application	Wordpress	Wordpress	4.7.1	All	All	All
Application	Wordpress	Wordpress	4.7.2	All	All	All
Application	Wordpress	Wordpress	4.7	All	All	All
Application	Wordpress	Wordpress	4.7.1	All	All	All
Application	Wordpress	Wordpress	4.7.2	All	All	All

cpe:2.3:a:wordpress:wordpress:4.7:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:4.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:4.7.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:4.7:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:4.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:4.7.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→