关于WordPress WPDB SQL注入漏洞的安全公告

**安全公告编号:CNTA-2017-0075**

近日，国家信息安全漏洞共享平台（CNVD）收录了WordPress WPDB SQL注入漏洞（CNVD-2017-32143）。远程攻击者利用该漏洞可造成SQL注入攻击，获取数据库敏感信息。漏洞的详细细节已公开，近期被不法分子利用进行大规模攻击尝试的可能性较大。

**一、漏洞情况分析**

WordPress是使用PHP语言和MySQL数据库开发的，世界上使用最广泛的博客系统，并逐步演化成一款内容管理软件。

2017年10月31日，WordPress官方发布了WordPress安全更新并修复了一处SQL注入漏洞，即$wpdb-prepare()函数可以创建无法预测且不安全的查询，从而导致潜在的SQL注入(SQLi)，但WordPress核心并不容易直接受到该漏洞的影响。CNVD对上述漏洞的综合评级为“高危”。

**二、漏洞影响范围**

漏洞影响WordPress 4.8.2及之前版本。

**三、漏洞修复建议**

支持自动更新的用户可以通过点击后台的仪表盘更新到4.8.3版本，也可手动下载更新：<https://wordpress.org/download/>

附：参考链接：

<https://wordpress.org/news/2017/10/wordpress-4-8-3-security-release/>

<https://blog.ircmaxell.com/2017/10/disclosure-wordpress-wpdb-sql-injection-technical.html>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32143>