预警编号：YJ-2017027

恒安嘉新

关于 WordPress WPDB SQL 注入漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 11 月 3 日

1 漏洞描述

近期 ,互联网爆出 WordPress WPDB SQL 注入漏洞(CVE-2017-11283),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出现大规模攻击尝试的可能性较大。漏洞危害程度为高危(High)。

2 影响范围

漏洞影响 WordPress 4.8.2 及之前版本

3 漏洞原理

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。

4 修复建议

目前，官方发布的安全更新，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。

另，不能后台更新的用户，建议可选择手动下载更新：

https://wordpress.org/download/