Wordpress SQLi

SQL Injections is an attack that uses an SQL query string to insert unsafe data, which can yield sensitive information or can be used to destroy databases. This exploit that was found on WordPress uses SQL injection that would allow the WordPress prepare function “$wpdb->prepare()” to create, or allow, SQL injections. The founder of the exploit, Anthony Ferrara, explained that the exploit was discovered after WordPress 4.8.2 was released. Charlie Osborne, of ZD Net, explained that patch 4.8.2 missed this issue and caused millions of lines of code to be compromised (Osborne 2017). Although he did not provide how the exploit was found, Ferrara did provide a quick overview of how the exploit should be patched. Ferrara explained that it would be best to remove the prepare function, however, it cannot be done quickly since it is a core function of WordPress. He further explained that WordPress may not be “always hackable” through the function, but this means that WordPress developers must constantly work on patches to prevent attacks while the prepare function is available. WordPress has taken the route of “hardening” their code to prevent any injections that could be made through themes or plugins.

References

Osborne, Charlie. “WordPress Patches SQL Injection Bug in Security Release.” ZDNet, ZDNet, 2 Nov. 2017, [www.zdnet.com/article/wordpress-patches-sql-injection-bug-in-emergency release/](http://www.zdnet.com/article/wordpress-patches-sql-injection-bug-in-emergency%09release/).

<https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/>