Privilege Escalation

Privilege Escalation is a type of exploitation that allows an attacker to do things that they should not do. For example, an administrator should be the only one with the capability to add or remove someone from a workgroup. Privilege escalation is when an attacker is able exploit a bug within a system that grants them those add/remove capabilities that should only be accessible to an administrator. Chris Brooke, an author from Threat Post, explained that there was an exploit that was found on WordPress that would utilize privilege escalation. The exploit gave attackers the capability to change the content of any Wordpress post or page; this could have been done on WordPress versions before 4.7.2 (Brook 2017). The exploit was found within the REST API that is being used by Word Press. REST API is an “architectural style” that deals with HTTP and its request methods (GET/POST, etc.). Marc-Alexandre Montpas, founder of the exploit, explained that the API preferred $\_GET and $\_POST values, which made the ID parameters quite dangerous(2017). An attacker could have submitted a request form with an ID such as **“/wp-json/wp/v2/posts/123?id=456ABC”, which would allow the attacker to manipulate a post with the ID set to 456 (Montpas 2017).** Montpas further explains that this could have allowed attackers to change a website’s page, spam the websites, install more plug-ins to widen the attack survive, and amongst other things. It was not specified how Word Press developers patched this

References

<https://restfulapi.net/>

Brook, Chris. “WordPress Silently Fixed Privilege Escalation Vulnerability in 4.72 Update.” Threatpost | The First Stop for Security News, 2 Feb. 2017, threatpost.com/wordpress-silently-fixed-privilege escalation-vulnerability-in-4-72-update/123533/.

Montpas, Marc-Alexandre. “Content Injection Vulnerability in WordPress 4.7 and 4.7.1.” Sucuri Blog, 8 Nov. 2017, blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress-rest-api.html.