Disastrous WordPress Rest API Bug – Inhibit Your WP Site from Being Hacked

Last month, WordPress patched three security issues out of four, covering a SQL injection vulnerability in WP-Query, the Press (for assigning taxonomy terms) and a cross-site scripting (XSS). The fourth and most disastrous security flaw that resided in WordPress REST API was disclosed with a delay of one week after its release. This delayed disclosure of vulnerability allowed several remote unauthorized hackers to modify the content of any page or post inside an unpatched WordPress site with the versions 4.7 and 4.7.1.

Reason for Delay:

Sucuri was working with the WordPress security team under that week to install the patch so that the security flaw was dealt with in short order before getting publicly disclosed.

As per the WordPress core contributor "Aaron Campbell" – "We believe transparency is in the public's best interest. It is our stance that security issues should always be disclosed. In this case, we intentionally delayed disclosing this issue by one week to ensure the safety of millions of additional WordPress sites."

"Data from all four WAFs and WordPress hosts showed no indication that the vulnerability had been exploited in the wild. As a result, we made the decision to delay disclosure of this particular issue to give time for automatic updates to run and ensure as many users as possible were protected before the issue was made public."

Disastrous WordPress Rest API Bug, Its Impacts and Results:

This security flaw has been rated as the most disastrous flaw and is now being actively exploited, even though the fix has automatically been deployed on millions of WP installations in the few hours once after the security patch was released. Hundreds of thousands of WordPress websites are seeing defacement with messages such as "Hacked by NG689Skw" or "Hacked by w4l3XzY3" or similar to these. You can also Google to know more about these specific hacks results that display

thousands of other hacked sites.

Solution to Inhibit Your WP Site from Being Hacked:

Therefore, all the WordPress admins who have their websites running 4.7.0 or 4.7.1 or not yet updated to 4.7.2, you are strongly recommended to update your CMS to 4.7.2 to avoid the risk of any content injection. If your site has already been defaced, simply update to the up-to-date version of WordPress and rollback your defaced posts to a review.

To know more about this vulnerability, you can head on the wptavern.com (**https://wptavern.com/wordpress-rest-api-vulnerability-is-being-actively-exploited-hundreds-of-thousands-of-sites-defaced**) or the official blog post of Sucuri (**https://blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress-rest-api.html**).