CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2019-004

WordPress Remote Code Execution

February 21, 2019 — v1.0

TLP:WHITE

History:

- *21/02/2019 — v1.0 – Initial publication*

Summary

A critical remote code execution vulnerability in versions of WordPress prior to 5.0.3 was disclosed. A flaw could be exploited by an attacker who gains access to an account with at least *author* privileges on a WordPress install to execute arbitrary PHP code on the underlying server.

Technical Details

The flaw is the chain of a **path traversal** and **local file inclusion** vulnerability that leads to remote code execution in the WordPress core and full remote takeover. Chaining the path traversal vulnerability with a local file inclusion flaw in theme directory could allow the attacker to execute arbitrary code on the targeted server.

The implementation of a security measure in WordPress versions 5.0.1 and 4.9.9 prevented the exploitation of the flaw because it made impossible for unauthorized users to set arbitrary post meta entries. However, the path traversal issue is still unpatched even in the latest WordPress version, it can also be exploited in presence of installed 3rd-party plugins that incorrectly handles Post Meta entries [3].

Products Affected

The vulnerability explained was rendered non-exploitable by a security patch in versions 4.9.9 and 5.0.1. However, the path traversal is still possible and currently unpatched.

Any WordPress site with a plugin installed that incorrectly handles post meta entries can make exploitation still possible.

Recommendations

It is highly recommended to upgrade to WordPress version 5.0.3. This should prevent from exploiting the remote code execution vulnerability. However, the remaining path traversal vulnerability will be addressed only with the next release.

References

[1] https://wordpress.org/news/2019/01/wordpress-5-0-3-maintenance-release

[2] https://blog.ripstech.com/2019/wordpress-image-remote-code-execution

[3] https://securityaffairs.co/wordpress/81393/hacking/wordpress-5-0-0-rce.html