FEYE-2021-0023

Description

The "WP Cerber" (wp-cerber) WordPress plugin before version 8.9.3 improperly checked certain HTTP parameters leading to an administrative multi-factor authentication bypass.

Impact

High - An attacker can access unintended information and functionality without completely authenticating.

Exploitability

Low - An attacker only requires a web browser to exploit this issue. However, the attacker requires knowledge of multi-factor bypasses techniques and would first have to compromise the user's username as well as password.

CVE Reference

CVE-2021-37597

Technical Details

When authenticating, the WordPress user is prompted to enter their 4-digit PIN code sent by email. However, it is possible to access pages and directories behind MFA without submitting the PIN code by modifying the HTTP request in the following ways:

- Deleting the `wordpress_logged_in_[hash]` cookie
- Removing a character from the `wordpress_logged_in_[hash]` cookie
- Adding a character to the `wordpress_logged_in_[hash]` cookie

Resolution

This issue was fixed as of version 8.9.3 of the WP Cerber plugin.

Discovery Credits

Ilyass El Hadi, Mandiant

Disclosure Timeline

- 28 July 2021 - Issue in "WP Cerber" reported to Wordpress
- 28 July 2021 - Wordpress acknowledged receipt of the report and that they were investigating
- 13 August 2021 - Follow-up on the issue requested to Wordpress
- 13 August 2021 - Wordpress confirms having contacted WP Cerber with a deadline to fix the issue
- 16 August 2021 - Version 8.9.3 of WP Cerber is released with a fix

References

WP Cerber Changelog