FEYE-2021-0024

Description

The "WP Cerber" (wp-cerber) WordPress plugin before version 8.9.3 improperly validated certain HTTP requests leading to a bypass of access controls on an API endpoint.

Impact

Low - Bypassing the access control list allows an unauthenticated attacker to extract data such as users, posts, authors, and IP addresses from the WordPress REST API. This information may inform attackers' follow-on analysis.

Exploitability

Medium - Exploiting this issue requires freely available proxy tools and a knowledge of common access control list bypass techniques.

CVE Reference

CVE-2021-37598

Technical Details

The Wordpress REST API endpoint located at `/wp-json`, by default, is blocked by WP Cerber from accessing its information. By appending a `?` to the endpoint as if to add a URL parameter, the access control list protections are bypassed and data can then be retrieved from the REST endpoint.

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