CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-005

Critical Vulnerabilities in WordPress Plugins

January 21, 2020 — v1.1

TLP:WHITE

History:

- *15/01/2020 — v1.0 – Initial publication*
- *21/01/2020 — v1.1 – Information on vulnerabilities found in another plugin added*

Summary

Critical vulnerabilities that are affecting two WordPress plugins have been identified [1, 4]. The vulnerabilities affect **InfiniteWP Client** and the **WP Time Capsule** plugins and allow a remote attacker to login into an administrator account without password. Vulnerabilities in **WP Database Reset** allowed any unauthenticated user to reset any table from the database to the initial WordPress set-up state.

Technical Details

Vulnerabilities in InfiniteWP Client and WP Time Capsule exist because of logical issues in both plugins affected. The plugins were missing authorization checks when handling a specially crafted POST request [2]. An attacker that could craft such POST requests would be logged in as an administrator without the need of password.

The database reset functions in the WP Database Reset plugin were not securely protected with capability checks or security nonces. Without proper security controls in place, the plugin contained a serious flaw that allowed any unauthenticated user the ability to reset any table in the database. This reset would result in a complete loss of data availability.

The InfiniteWP Client, WP Time Capsule, and WP Database Reset have according to [3] respectively 300k, 20k, and 80k installations.

Affected Products

List of all affected products:

- InfiniteWP Client prior to version 1.9.4.5
- WP Time Capsule prior to version 1.21.16
- WP Database Reset prior to version 3.15

Recommendations

It is recommended to update these plugins to the latest version as soon as possible.

References

[1] https://www.theregister.co.uk/2020/01/15/update_wordpress_plugins/

[2] https://www.webarxsecurity.com/vulnerability-infinitewp-client-wp-time-capsule/

[3] https://wordpress.org/plugins/browse/popular/

[4] https://www.wordfence.com/blog/2020/01/easily-exploitable-vulnerabilities-patched-in-wp-database-reset-plugin/