CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-008

# WordPress Profile Builder Plugin Critical Vulnerability

*February 18, 2020 — v1.0*

**TLP:WHITE**

*History:*

- *18/02/2020 — v1.0 – Initial publication*

## Summary

A critical vulnerability affecting the WordPress Profile Builder Plugin has been identified [1, 2]. Profile Builder is a plugin designed to create custom forms that allow users to register, edit their profile, etc. The plugin is affected by a broken authentication vulnerability, allowing unauthenticated users to register or edit their account and gain *Administrator* privileges using the plugin's form. It is estimated that around 50K sites are running the free version of Profile Builder and around 15k the Pro and Hobbyist version.

## Technical Details

The plugin features a custom user role editor that allows admins to assign custom sets of privileges to their site's users [2]. Due to a bug in the form handler, it is possible for an attacker to submit input on form fields that doesn't exist in the actual form. Specifically, if the site's administrator has not added the `User Role` field to the form, an attacker could still inject a user role value into their form submission.

When an administrator adds the `User Role` selector to a form, a list of approved roles must be selected for new users. If this list is created, only approved roles will be accepted by the form handler. However, when the `User Role` field is not present and an attacker submits a user role anyway, there is no list of approved roles and any input is accepted.

Combining the two issues will allow unauthenticated attackers to register `Administrator` accounts on WordPress sites running the vulnerable plugin.

## Products Affected

List of all affected products:

- Profile Builder version 3.1.0 or before
- Profile Builder Pro version 3.1.0 or before

## Recommendations

It is recommended to update the plugin to the latest version as soon as possible. This vulnerability has been fixed in version 3.1.1.

## References

[1] https://wpvulndb.com/vulnerabilities/10066

[2] https://www.wordfence.com/blog/2020/02/critical-vulnerability-in-profile-builder-plugin-allowed-site-takeover/