Security Advisory 2023-032

Vulnerability in Wordpress Gravity Forms Plugin

May 31, 2023 — v1.0

TLP:CLEAR

History:

- *31/05/2023 — v1.0 – Initial publication*

Summary

On May 30, 2023, an unauthenticated PHP Object Injection vulnerability has been discovered in the Wordpress' Gravity Forms plugin. This vulnerability, identified as CVE-2023-28782 (CVSS score of 8.3), may allow an unauthenticated user to pass ad-hoc serialised strings to a vulnerable `unserialize` call, resulting in an arbitrary PHP object(s) injection into the application scope [1].

This vulnerability could be triggered in a default installation of the Gravity Forms plugin and only needs a form that contains a list field.

Technical Details

The Gravity Forms plugin vulnerability occurs when user-supplied input is not properly sanitised before being passed to the `maybe_unserialize` function which is a wrapper for PHP `unserialize` function.

The vulnerability is found within the `get_field_input` function in the file:

```
includes/fields/class-gf-field-list.php
```

which handles the input field processing of a list field on Gravity Forms. There is also a legacy `get_legacy_field_input` function which has identical code that is also vulnerable.

The input value comes from the `$value` variable, since there is no proper check or sanitisation on the variable and the `$value` variable is directly passed to the `maybe_unserialize` function, any unauthenticated user is able to trigger PHP object injection by submitting to a list field on the form created from the Gravity Forms plugin.

The `get_field_input` function from the list field could be called from the `get_field_input` function located in `common.php` which would then act as an initial handler of input and would forward the process to each field function handler.

Affected Products

The affected product is:

- Gravity Forms plugin version 2.7.3 and below.

Recommendations

To mitigate this vulnerability, users should update the respective plugins to at least version 2.7.4.

References

[1] https://patchstack.com/articles/unauthenticated-php-object-injection-in-gravity-forms-plugin/

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28782