CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-007

Vulnerabilities in WordPress GDPR Cookie Consent Plugin

February 14, 2020 — v1.0

TLP:WHITE

History:

- *14/02/2020 — v1.0 – Initial publication*

Summary

Critical vulnerabilities affecting the WordPress GDPR Cookie Consent plugin have been identified. This plugin is used to make websites GDPR compliant. The vulnerability was reported by the security researcher Jerome Bruandet from NinTechNet [1, 2]. The exploitation of the vulnerabilities lead to **privilege escalation** and **authenticated stored XSS**. This plugin has 700k active installs.

Technical Details

An AJAX endpoint used in the administration pages of the plugin is the cause of the problem. It fails to implement checks, and as result three actions were exposed: `get_policy_pageid`, `autosave_contant_data`, and `save_contentdata`.

Authenticated Stored XSS

The `autosave_contant_data` is intended to define the default content that appears in the cookie policy preview page. It saves the data into the `cli_pg_content_data` database field without validating it. An authenticated user can use it to inject JavaScript code, which will be loaded and executed each time someone – authenticated or not – visits the `http[:]//example[.]com/cli-policy-preview/` page.

Privilege Escalation

The `save_contentdata` method allows the administrator to save the GDPR cookie notice to the database as a page post type. An authenticated user, such as a subscriber, can use it to put any existing page or post (or event the entire website) offline by changing their status from *published* to *draft*. Additionally, it is possible to delete or change their content. Injected content can include formatted text, local or remote images, as well as hyperlinks and shortcodes. The technique is explained in depth in [2 and 3].

Affected Products

List of all affected products:

- WordPress GDPR Cookie Consent plugin version 1.8.2 or below

Recommendations

It is recommended to update the plugin to the latest version as soon as possible. This vulnerability has been fixed in version 1.8.3.

References

[1] https://wordpress.org/plugins/cookie-law-info/

[2] https://blog.nintechnet.com/wordpress-gdpr-cookie-consent-plugin-fixed-vulnerability/

[3] https://www.wordfence.com/blog/2020/02/improper-access-controls-in-gdpr-cookie-consent-plugin/