NinTechNet

The Ninja Technologies Network

MENU

Unauthenticated stored XSS and content spoofing vulnerabilities in WordPress WP GDPR plugin (unpatched).

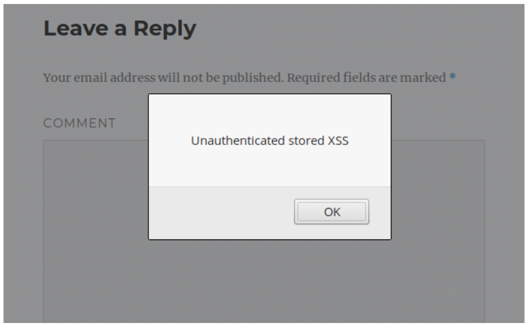
BY JEROME BRUANDET APRIL 23, 2020 - 10:54AM [+0700]

> This plugin is not maintained any longer and the vulnerability has never been fixed. Make sure to follow the recommendations below.

The WordPress WP GDPR plugin, which has 6,000+ active installations, is prone to multiple vulnerabilities affecting version 2.1.1 and below.

Improper access control and unvalidated user input can lead to:

- Stored XSS: An unauthenticated attacker can inject JavaScript code that will be triggered when someone accesses a page or post that has a comment form:



Leave a Reply

Your email address will not be published. Required fields are marked *

Unauthenticated stored XSS

- Content Spoofing: An unauthenticated attacker can gain full control over the WordPress `comments` table in the database and can tamper with any of its 14 fields: change the content of all comments, assign them to another user or to another post, bypass moderation/approval etc.

- Additional issue: An unauthenticated attacker can delete any comment as well as modify the plugin's settings.

Because all issues are unfixed we won't provide more details.

Timeline

The vulnerability was reported to the wordpress.org team on October 22, 2019 and the plugin was removed from the repo.

Recommendations

We recommend to uninstall this plugin as there isn't any security patch available. If you are using our web application firewall for WordPress, NinjaFirewall WP Edition (free) and NinjaFirewall WP+ Edition (premium), you are protected against this vulnerability since October 2019.

Stay informed about the latest vulnerabilities

- Running WordPress? You can get email notifications about vulnerabilities in the plugins or themes installed on your blog.
- On Twitter: @nintechnet

TAGGED: NINJAFIREWALL, SECURITY, VULNERABILITY, WORDPRESS

PREVIOUS
WordPress Ultimate Addons for Gutenberg plugin fixed vulnerability.

NEXT
Authenticated settings change vulnerability in WordPress Quick Page/Post Redirect plugin (unpatched).

Code Profiler

Speed up your WordPress website by locating bottlenecks and performance issues in your plugins and themes.

FREE DOWNLOAD

CATEGORIES

Select Category

SEARCH

Search …

RECENT POSTS

1. WordPress FlyingPress plugin fixed broken access control vulnerability.
   November 28, 2022 - 12:13pm [+0700]
2. 8 WordPress plugins fixed high severity vulnerability.
   April 12, 2022 - 11:48am [+0700]
3. Unauthenticated function injection vulnerability in WordPress Sparkling theme.
   February 10, 2022 - 5:41pm [+0700]
4. Critical vulnerability in WordPress AdSanity plugin.
   January 25, 2022 - 12:17pm [+0700]
5. Code Profiler: WordPress Website Performance Profiling Made Easy.
   December 19, 2021 - 1:48am [+0700]