WordPress Membership Plugin Flaw Exposes Sensitive Stripe Data via @sejournal, @martinibuster

An advisory was published about a vulnerability discovered in the Membership Plugin By StellarWP which exposes sensitive Stripe payment setup data on WordPress sites using the plugin. The flaw enables unauthenticated attackers to launch attacks and is rated 8.2 (High).

Membership Plugin By StellarWP

The Membership Plugin – Restrict Content By StellarWP is used by WordPress sites to manage paid and private content. It enables site owners to restrict access to pages, posts, or other resources so that only logged-in users or paying members can view them and manage what non-paying site visitors can see. The plugin is commonly deployed on membership and subscription-based sites.

Vulnerable to Unauthenticated Attackers

The Wordfence advisory states that the vulnerability can be exploited by unauthenticated attackers, meaning no login or WordPress user account is required to launch an attack. User permission roles do not factor into whether the issue can be triggered, and that’s what makes this particular vulnerability more dangerous because it’s easier to trigger.

What the Vulnerability Is

The issue stems from missing security checks related to Stripe payment handling. Specifically, the plugin failed to properly protect Stripe SetupIntent data.

A Stripe SetupIntent is used during checkout to collect and save a customer's payment method for future use. Each SetupIntent includes a client_secret value that is intended to be shared during a checkout or account setup flow.

The official Wordfence advisory explains:

> *"The Membership Plugin – Restrict Content plugin for WordPress is vulnerable to Missing Authentication in all versions up to, and including, 3.2.16 via the 'rcp_stripe_create_setup_intent_for_saved_card' function due to missing capability check.*
>
> *Additionally, the plugin does not check a user-controlled key, which makes it possible for unauthenticated attackers to leak Stripe SetupIntent client_secret values for any membership."*

According to Stripe's official documentation, the Setup Intents API is used to set up a payment method for future charges without creating an immediate payment. A SetupIntent includes a client_secret. Stripe's documentation states that client_secret values should not be stored, logged, or exposed to anyone other than the intended customer.

This is how Stripe's documentation explains what the purpose is for the Setup Intents API:

> *"Use the Setup Intents API to set up a payment method for future payments. It's similar to a payment, but no charge is created.*

> *The goal is to have payment credentials saved and optimized for future payments, meaning the payment method is configured correctly for any scenario. When setting up a card, for example, it may be necessary to authenticate the customer or check the card's validity with the customer's bank. Stripe updates the SetupIntent object throughout that process."*

Stripe documentation also explains that client_secret values are used client-side to complete payment-related actions and are intended to be passed securely from the server to the browser. Stripe states that these values should not be stored, logged, or exposed to anyone other than the relevant customer.

This is how Stripe's documentation explains the client_secret value:

> *"client_secret*
> *The client secret of this Customer Session. Used on the client to set up secure access to the given customer.*
>
> *The client secret can be used to provide access to customer from your frontend. It should not be stored, logged, or exposed to anyone other than the relevant customer. Make sure that you have TLS enabled on any page that includes the client secret."*

Because the plugin did not enforce the appropriate protections, Stripe SetupIntent client_secret values could be exposed.

What this means in real life is that Stripe payment setup data associated with memberships was accessible beyond its intended scope.

Affected Versions

The vulnerability affects all versions of the plugin up to and

including version 3.2.16. Wordfence assigned the issue a CVSS score of 8.2, reflecting the sensitivity of the exposed data and the fact that no authentication is required to trigger the issue.

A score in this range indicates a high-severity vulnerability that can be exploited remotely without special access, increasing the importance of timely updates for sites that rely on the plugin for managing paid memberships or restricted content.

Patch Availability

The plugin has been updated with a patch and is available now. The issue was fixed in version 3.2.17 of the plugin. The update adds missing nonce and permission checks related to Stripe payment handling, addressing the conditions that allowed SetupIntent client_secret values to be exposed. A nonce is a temporary security token that ensures a specific action on a WordPress website was intentionally requested by the user and not by a malicious attacker.

The official Membership Plugin changelog responsibly discloses the updates:

> *“3.2.17*
> *Security: Added nonce and permission checks for adding Stripe payment methods.*
> *3.2.16*
> *Security: Improved escaping and sanitization for [restrict] and [register_form] shortcode attributes.”*

What Site Owners Should Do

Sites using Membership Plugin – Restrict Content should update to version 3.2.17 or newer.

Failure to update the plugin will leave the Stripe SetupIntent client_secret data exposed to unauthenticated attackers.

Featured Image by Shutterstock/file404

https://www.searchenginejournal.com/wordpress-membership-plugin-flaw-exposes-sensitive-stripe-data/565124/