Formidable Forms Flaw Lets Attackers Pay Less For Expensive Purchases via @sejournal, @martinibuster

A vulnerability in the Formidable Forms WordPress plugin installed on over 300,000 websites enables unauthenticated attackers to bypass payment verification. The vulnerability affects all versions up to and including 6.28. It makes it possible for attackers to reuse a Stripe payment made for a lower amount to mark a more expensive transaction as paid.

Formidable Forms Plugin

The Formidable Forms plugin is a drag-and-drop form builder used by WordPress sites to create contact forms, surveys, registration forms, and payment forms. Sites use it with payment processors (like PayPal and Stripe) to collect payments for services, memberships, digital products, and event registrations.

Vulnerable To Unauthenticated Attackers

What makes this vulnerability especially concerning is that it does not require authentication. An attacker does not need to log in or obtain even subscriber-level access to exploit the flaw. This makes it easier for attackers to take advantage of the payment validation weakness.

The vulnerability has been assigned CVE-2026-2890 and carries a CVSS severity score of 7.5/10, which is rated High.

Payment Integrity Bypass

The vulnerability is due to missing validation in the handle_one_time_stripe_link_return_url function. The function marks payment records as complete based solely on the Stripe PaymentIntent status. This makes it possible for attackers to reuse a valid PaymentIntent for a smaller charge to approve a more expensive purchase.

The verify_intent() function validates only that the client secret belongs to the user. It does not bind the PaymentIntent to a specific form submission. It does not verify that the amount charged matches the amount the customer was supposed to pay.

According to Wordfence:

> *“The Formidable Forms plugin for WordPress is vulnerable to a payment integrity bypass in all versions up to, and including, 6.28. This is due to the Stripe Link return handler (`handle_one_time_stripe_link_return_url`) marking payment records as complete based solely on the Stripe PaymentIntent status without comparing the intent’s charged amount against the expected payment amount, and the `verify_intent()` function validating only client secret ownership without binding intents to specific forms or actions.*
>
> *This makes it possible for unauthenticated attackers to reuse a PaymentIntent from a completed low-value payment to mark a high-value payment as complete, effectively bypassing payment for goods or services.”*

This makes it possible for unauthenticated attackers to complete a small low-cost transaction and then reuse that

PaymentIntent to approve a more expensive transaction without paying the full price.

This vulnerability does not enable remote code execution or direct server compromise. But it does enable attackers to obtain goods or services without paying the required price.

Affected Versions And Patch

All versions up to and including 6.28 are affected. Users of the Formidable Forms plugin are encouraged by Wordfence to update to version 6.29 or newer to address the vulnerability.

https://www.searchenginejournal.com/formidable-forms-flaw-lets-attackers-pay-less-for-expensive-purchases/569665/