مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in WPForms Plugin

Tracking #:432316610
Date:10-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the popular WPForms WordPress plugin that could allow authenticated attackers to perform unauthorized actions on Stripe payments, such as refunds and cancellations.

TECHNICAL DETAILS:

A high-severity vulnerability (CVE-2024-11205) exists in the popular WPForms plugin, potentially impacting over 6 million WordPress websites. This security flaw allows authenticated attackers with subscriber-level access or higher to perform unauthorized Stripe payment refunds and subscription cancellations.

Vulnerability Details:

- **CVE-2024-11205**
- CVSS Score: 8.5 (High)
- The vulnerability stems from a missing capability check in the wpforms_is_admin_page function, which is used by the ajax_single_payment_refund() and ajax_single_payment_cancel() functions. Although these functions are nonce-protected, attackers can obtain the necessary nonce to bypass this protection.
- Successful Exploitation of this vulnerability can lead to:
  - Unauthorized refunds of Stripe payments
  - Cancellation of active Stripe subscriptions
  - Potential revenue loss for affected businesses
  - Disruption of subscription services
  - Increased administrative burden
- **Plugin:** WPForms - Easy Form Builder for WordPress
- **Affected Versions:** 1.8.4 to 1.9.2.1
- **Fixed Versions:** 1.9.2.2 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.wordfence.com/blog/2024/12/6000000-wordpress-sites-protected-against-payment-refund-and-subscription-cancellation-vulnerability-in-wpforms-wordpress-plugin/