Ameaça crítica do SQLi para usuários do plug-in de associações do WordP

Data: 2025-09-04 11:09:07

Autor: Inteligência Against Invaders

Um sério problema de segurança foi descoberto no plug-in WordPress Paid Membership

Subscriptions, que é usado por mais de 10.000 sites para gerenciar assinaturas e pagamentos

recorrentes.

As versões 2.15.1 e anteriores são afetadas por uma vulnerabilidade de injeção de SQL não autenticada, rastreada como CVE-2025-49870.

A falha permite que invasores injetem consultas SQL maliciosas no banco de dados sem exigir credenciais de login.

O pesquisador da Patchstack Alliance, ChuongVN, identificou o problema e confirmou que ele foi resolvido na versão 2.15.2.

Como funciona a vulnerabilidade

O bug decorre da maneira como o plug-in lida com as notificações de pagamento instantâneo do PayPal (IPN).

Quando uma transação é processada, o plug-in extrai um ID de pagamento diretamente dos dados fornecidos pelo usuário e o insere em uma consulta de banco de dados sem a devida validação.

Ao manipular essa entrada, os invasores podem obter acesso não autorizado a informações confidenciais ou modificar registros armazenados.

Leia mais sobre vulnerabilidades de injeção de SQL: CISA e FBI pedem esforços renovados para eliminar falhas de injeção de SQL

Para resolver o problema, os desenvolvedores fizeram várias alterações na versão 2.15.2, incluindo:

- Garantir que o ID de pagamento seja numérico antes do uso
- Substituindo a concatenação de consulta vulnerável por instruções preparadas
-

As instruções preparadas impedem que os invasores alterem a estrutura pretendida das consultas de banco de dados, eliminando o risco de injeção.

Riscos de injeção de SQL

A injeção de SQL tem sido um dos problemas de segurança da Web mais perigosos devido ao seu potencial de comprometer bancos de dados inteiros.

Como uma pilha de retalhos Consultivo observou: “para o processo de consulta SQL, sempre faça uma fuga segura e formate a entrada do usuário antes de executar uma consulta. A melhor prática é sempre usar uma instrução preparada e também converter cada uma das variáveis usadas para o uso pretendido.”

Os usuários de plug-ins são fortemente aconselhados a atualizar para a versão 2.15.2 o mais rápido possível para proteger seus sites contra exploração.