Una vulnerabilidad de día cero en la última versión de un plugin premium de WordPress conocido como WPGateway se está explotando activamente en la naturaleza, lo que podría permitir que los hackers se apoderen completamente de los sitios web afectados.

Rastreada como CVE-2022-3180 (puntaje CVSS: 9.8), la vulnerabilidad se está armando para agregar un usuario administrador malicioso a los sitios que ejecutan el complemento WPGateway, dijo la compañía de seguridad de WorDPress, Wordfence.

> *«Parte de la funcionalidad del complemento expone una vulnerabilidad que permite a los atacantes no autenticados insertar un administrador malicioso»,* dijo Ram Gall, investigador de Wordfence.

WPGateway se factura como un medio para que los administradores del sitio instalen, respalden y clonen plugins y temas de WordPress desde un tablero unificado.

El indicador más común de que un sitio web que ejecuta el plugin se ha visto comprometido es la presencia de un administrador con el nombre de usuario *«rangex»*.

Además, la aparición de solicitudes a *«/wp-content/plugins/wpgateway/wpgateway-webservice-new.php?wp_new_credentials=1»* en los registros de acceso es una señal de que el sitio de WordPress ha sido atacado usando la vulnerabilidad, aunque no implica de forma necesaria una violación exitosa.

Wordfence dijo que bloqueó más de 4.6 millones de ataques que intentaron aprovechar la vulnerabilidad contra más de 280,000 sitios en los últimos 30 días.

Se retuvieron más detalles sobre la vulnerabilidad debido a la explotación activa y para evitar que otros atacantes se aprovechen de la deficiencia. En ausencia de un parche, se recomienda a los usuarios que eliminen el plugin de sus instalaciones de WordPress hasta que haya una solución disponible.

El desarrollo se produce días después de que Wordfence advirtiera sobre el abuso en la naturaleza de otra vulnerabilidad de día cero en un plugin de WordPress llamado BackupBuddy.

La divulgación también llega cuando Sansec reveló que los atacantes irrumpieron en el sistema de licencias de extensión de FishPig, un proveedor de integraciones populares de Magento-WordPress, para inyectar un código malicioso diseñado para instalar un troyano de acceso remoto llamado Rekoobe.