Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Vulnerabilidad de día cero en WPGateway explotada activamente en estado salvaje.

14/Septiembre/2022

Contenido

INTRODUCCIÓN

Un plugin utilizado en Wordpress ha sido vulnerado por un día cero encontrado en sus ultimas versiones, hablamos de WPGateway.

Día Cero en Plugin WPGateway

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_09_14_01
Clasificación de alerta:	Vulnerabilidad
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/14/2022
Es día cero (0 day):	Si

Resumen

El 8 de septiembre de 2022, el equipo de Wordfence Threat Intelligence se dio cuenta de una vulnerabilidad de día cero explotada activamente que se usaba para agregar un usuario administrador malicioso a los sitios que ejecutan el complemento WPGateway. Publicaron una regla de firewall para los clientes de Wordfence Premium, Wordfence Care y Wordfence Response para bloquear el exploit el mismo día, 8 de septiembre de 2022.

Los sitios que todavía ejecutan la versión gratuita de Wordfence recibirán la misma protección 30 días después, el 8 de octubre de 2022. El cortafuegos de Wordfence ha bloqueado con éxito más de 4,6 millones de ataques dirigidos a esta vulnerabilidad contra más de 280 000 sitios en los últimos 30 días.

Detalles de la Vulnerabilidad

Descripción: Escalada de privilegios no autenticada Complemento
afectado: WPGateway
Plugin Slug: wpgateway
Desarrollador del complemento: Jack Hopman/WPGateway
Versiones afectadas: <= 3.5
ID de CVE: CVE-2022-3180
Puntaje de CVSS: 9.8 (crítico)
Vector de CVSS: CVSS:3.1/AV: N/AC:L/PR:N/UI:N/ S:U/C:H/I:H/A:H
Versión totalmente parcheada: N/A

El complemento WPGateway es un complemento premium vinculado al servicio en la nube WPGateway, que ofrece a sus usuarios una forma de configurar y administrar sitios de WordPress desde un único panel. Parte de la funcionalidad del complemento expone una vulnerabilidad que permite a los atacantes no autenticados insertar un administrador malicioso.

Si bien Wordfence reveló la explotación activa de este error de seguridad, no publicó información adicional sobre estos ataques ni detalles sobre la vulnerabilidad.

Al ocultar esta información, Wordfence dice que quiere evitar una mayor explotación. Es probable que esto también permita que más clientes de WPGateway parcheen sus instalaciones antes de que otros atacantes desarrollen sus propias vulnerabilidades y se unan a los ataques.

Como saber si su sitio fue vulnerado.

Si está trabajando para determinar si un sitio se ha visto comprometido con esta vulnerabilidad, el indicador más común de compromiso es un administrador malicioso con el nombre de usuario: rangex.

Si ve a este usuario agregado a su tablero, significa que su sitio ha sido comprometido.

Además, puede consultar los registros de acceso de su sitio en busca de solicitudes para:
//wp-content/plugins/wpgateway/wpgateway-webservice-new.php?wp_new_credentials=1

Si estas solicitudes están presentes en sus registros, indican que su sitio ha sido atacado mediante un exploit dirigido a esta vulnerabilidad, pero no necesariamente indican que se haya comprometido con éxito.

Recomendaciones

- Si tiene instalado el complemento WPGateway, le recomendamos que lo elimine de inmediato hasta que haya un parche disponible.

- Verifique si hay usuarios administradores maliciosos en su panel de WordPress.

- Si cree que su sitio se ha visto comprometido como resultado de esta vulnerabilidad o cualquier otra vulnerabilidad, reportar incidentes a través de Wordfence Care.

Noticia Completa

https://devel.group/blog/dia-cero-en-plugin-wpgateway/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente