USTIC-AV 12/22. Vulnerabilidad grave en complemento de WordPress (19/09/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones avisa de la **publicación de una vulnerabilidad grave,** de **"día cero**" (*Zero day*), **en** la última versión de un complemento premium de **WordPress** conocido como WPGateway **que se está explotando activamente**, **lo que podría permitir que los actores malintencionados se apoderen por completo de los sitios afectados.**

Detalle

Registrada como CVE-2022-3180 (puntuación CVSS: 9.8), se trata de una vulnerabilidad de “día cero” que **permite a los atacantes no autenticados agregar un usuario malicioso con privilegios de administrador a sitios web basados en WordPress que ejecutan el complemento premium WPGateway**, tal como ha anunciado Wordfence, proveedor de soluciones de ciberseguridad del citado CMS.

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

El indicador más común de que un sitio web que ejecuta el complemento se ha visto comprometido es la presencia de un administrador con el nombre de usuario ***"rangex"***. Además, si los logs de la página muestran accesos a '*/plugins/wpgateway /wpgateway-webservice-new.php?wp_new_credentials=1'*, significa que ha sido atacada, pero no necesariamente que esté comprometida

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.

De acuerdo con la información publicada, **esta vulnerabilidad está siendo explotada activamente por atacantes remotos**, lo que se traduce en un escenario de riesgo, por lo que rogamos encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente a las vulnerabilidades.

Recursos Afectados

- Sitios web basados en WordPress que ejecutan el complemento premium WPGateway

Recomendaciones Actualizadas (19/09/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas:

Mitigación

1º. Solución a las vulnerabilidades:

- **Eliminar** el plugin **WPGateway** hasta que se libere un parche de seguridad.

Referencias

- **Publicaciones sobre la vulnerabilidad:**
  - https://thehackernews.com/2022/09/over-280000-wordpress-sites-attacked.html
  - https://www.genbeta.com/seguridad/tu-web-wordpress-tiene-nuevo-usuario-este-nombre-cientos-miles-victimas-grave-vulnerabilidad
  - https://blog.elhacker.net/2022/09/grave-vulnerabilidad-WPGateway-WordPress.html

---

En caso de haber detectado la explotación de estas vulnerabilidades :

debe reportar el incidente mediante correo electrónico a sau.cges.sspa@juntadeandalucia.es indic ando en el *Asunto: [Compromiso WordPress0922]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud