Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 049	Fecha: 25-02-2023
		Página 4 de 7

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidad en complemento de WordPress		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	ECV
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

Se ha detectado una vulnerabilidad de SQL Injection en un complemento de WordPress.

ANTECEDENTES:

- WordPress, es un sistema de gestión de contenidos (CMS) que se compone de un servidor web: Core, Temas y Plugins, con estos componentes se puede crear contenidos web.

- El complemento de WordPress ReviewX, permite establecer criterios para la revisión de un producto; en su versión gratuita, los criterios son limitados.

- Con fecha 20 de enero del presente año, fueron publicadas tres vulnerabilidades de SQL Injection correspondientes a los siguientes complementos de WordPress

    - Paid Memberships Pro (CVE-2023-23488).
    - Easy Digital Downloads (CVE-2023-23489).
    - Survey Maker (CVE-2023-23490).

DETALLES:

- La acción 'rx_export_review' en el complemento de WordPress ReviewX versión < 1.6.4, se ve afectada por una vulnerabilidad de SQL Injection en los parámetros 'filterValue' y 'selectedColumns'.

- La vulnerabilidad requiere que el atacante esté autenticado, pero no requiere privilegios de administrador.

- Se puede usar un comando curl simple para demostrar el problema (se requiere una cookie de sesión de WordPress válida o actual). En el siguiente comando, el parámetro "$TARGET_HOST" se reemplaza con la instancia de WordPress de destino y "$WP_COOKIE" con el encabezado completo de la cookie para un usuario de WordPress que haya iniciado sesión.

  Curl "http://$TARGET_HOST/wp-admin/admin-ajax.php" --header "$WP_COOKIE" --data "action=rx_export_review&filterValue[6]=&filterValue[7]=id&selectedColumns[]=1+AND+(SELECT+1+FROM+(SELECT(SLEEP(1)))a)"

- La vulnerabilidad fue registrada con el código **CVE-2023-26325**

RECOMENDACIONES:

- Actualizar el complemento ReviewX de WordPress, a la versión 1.6.4.
- Actualizar las contraseñas regularmente para reducir el riesgo de un ataque.
- Implementar políticas privilegios mínimos tanto para empleados como para proveedores.
- Evitar descargar aplicaciones de sitios no confiables.
- Mantenerse informado sobre alertas de brechas de seguridad que afecten a los proveedores.
- Mantener al sistema operativo, programa y antivirus con las ultimas actualizaciones.

Fuentes de información	▪ hxxps://www.tenable.com/security/research/tra-2023-2 ▪ Análisis propio de fuentes abiertas.