| | | |
|---|---|---|
| DINI | **ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°245** | **Fecha: 16-10-2023** |
| | | **Página: 11 de 15** |

| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN NACIONAL DE INTELIGENCIA** | | |
| Nombre de la alerta | Múltiples vulnerabilidades en el sistema de gestión de contenidos “WordPress” | | |
| Tipo de Ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Red, Internet | | |
| Código de familia | H | Código de Sub familia | H01 |
| Clasificación temática familia | Intento de intrusión | | |

Descripción

**1. ANTECEDENTES:**

Se ha reportado múltiples vulnerabilidades de severidad **ALTA** y **MEDIA** de tipo deserialización de datos que no son de confianza, inyección de código y secuencia de comandos entre sitios (XSS) en el sistema de gestión de contenidos WordPress. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar códigos cortos arbitrarios, robar información confidencial, cambiar la apariencia de la página web, realizar ataques de phishing y realizar ataques de descarga automática.

**2. DETALLES:**

La vulnerabilidad de severidad **alta** de tipo deserialización de datos que no son de confianza, existe debido a una validación de entrada insegura al procesar datos serializados. Un usuario remoto puede pasar datos especialmente diseñados a la aplicación y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad de severidad **media** de tipo inyección de código, existe debido a una validación de entrada incorrecta. Un usuario remoto puede eludir las restricciones de seguridad implementadas y ejecutar códigos cortos arbitrarios en el sitio web.

La vulnerabilidad de severidad **media** de tipo secuencia de comandos entre sitios, existe debido a una limpieza insuficiente de los datos proporcionados por el usuario pasados a través de los parámetros Success_url y Rechace_url en la pantalla de contraseña de la aplicación. Un atacante remoto puede engañar a la víctima para que siga un enlace especialmente diseñado y ejecute código HTML y script arbitrario en el navegador del usuario en el contexto de un sitio web vulnerable.

**A. Productos afectados:**

- WordPress: 5.6 - 6.3.1.

**3. RECOMENDACIÓN:**

- Actualizar el producto afectado a la version 6.3.2 que aborda esta vulnerabilidad. Esta versión de ciclo corto de seguridad y mantenimiento presenta 19 correcciones de errores en Core , 22 correcciones de errores para el Editor de bloques y 8 correcciones de seguridad. Cabe indicar que el próximo lanzamiento importante será la versión 6.4 prevista para el 7 de noviembre de 2023.

| | |
|---|---|
| Fuente de Información: | • hxxp://wordpress.org/news/2023/10/wordpress-6-3-2-maintenance-and-security-release/<br>• hxxp://wpscan.com/vulnerability/da1419cc-d821-42d6-b648-bdb3c70d91f2/ |