Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA21-00435-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	03 de mayo de 2021
Última revisión	03 de mayo de 2021

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre dos vulnerabilidades en WordPress.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-29447
CVE-2021-29450

Impactos

Ambas vulnerabilidades son caracterizadas como de riesgo medio.

CVE-2021-29447: Esta vulnerabilidad permite a un usuario remoto ganar acceso a información sensible. Tiene lugar debido a validación insuficiente del input XML en la biblioteca Media. Un atacante remoto autenticado con la habilidad de subir archivos puede enviar un código XML especialmente diseñado y ver contenido de archivos arbitrarios en el sistema o iniciar solicitudes a sistemas externos.

CVE-2021-29450: Esta vulnerabilidad existe debido a la aplicación no adecuada de las restricciones de seguridad dentro de la implementación REST API, y permite a un usuario remoto ganar acceso a información sensible.

Productos Afectados
WordPress, versiones de la 4.7 a la 5.7.

Mitigación
Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces
https://wordpress.org/news/category/security/
https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-rv47-pc52-qrhh
https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-pmmh-2f36-wvhq
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29447
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29450

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.03 18:24:47 -04'00'