Alerta de seguridad cibernética	9VSA22-00728-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de octubre de 2022
Última revisión	19 de octubre de 2022

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 CSIRT de Gobierno. 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 vulnerabilidades que son parchadas en la nueva versión de Wordpress.

Vulnerabilidades

Son 15, todas con CVE pendiente.

Impacto

Vulnerabilidades de riesgo alto

CVE Pendiente: Cross-Site Scripting reflejado, via inyección SQL en Media Library.
CVE Pendiente: Ataque XSS a través de wp-mail[.]php
CVE Pendiente: Inyección SQL via WP_Date_Query
CVE Pendiente. Falsificación XSS via wp-trackback[.]php

Productos afectados

Wordpress anteriores al 6.0.3.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
https://www.wordfence.com/blog/2022/10/patch-now-the-wordpress-6-0-3-security-update-contains-important-fixes/

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.10.19 14:44:45 -03'00'