Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00698-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de agosto de 2022
Última revisión	31 de agosto 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 nuevas vulnerabilidades que afectan a productos de Wordpress.

Vulnerabilidades

CVE pendiente
CVE pendiente
CVE pendiente

Impacto

Vulnerabilidades de alto riesgo

La vulnerabilidad de mayor riesgo requiere privilegios administrativos y no es fácil de explotar en las configuraciones por defecto, pero puede haber plugins o temas (themes) que permita que sea detonada por usuarios con menores privilegios (como a nivel de editor y menores).

Productos afectados

WordPress Content Management System (CMS), versiones anteriores a la 6.0.2 (la versión 6.0.2 parcha las vulnerabilidades contenidas en este documento).

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.08.31 12:21:16 -04'00'

Enlaces

https://www.wordfence.com/blog/2022/08/wordpress-core-6-0-2-security-maintenance-release-what-you-need-to-know/