

Alerta de seguridad cibernética	9VSA21-00489-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de septiembre de 2021
Última revisión	13 de septiembre 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 afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre la actualización 5.8.1 de WordPress.

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

Vulnerabilidades

CVE-2021-39200
CVE-2021-39201
CVE-2021-39202
CVE-2021-39203

Impactos

CVE-2021-39200: Riesgo medio. Esta vulnerabilidad permite a un atacante remoto ganar acceso a información potencialmente sensible, debido a un output excesivo de datos por la aplicación en la función "wp_die()".

CVE-2021-39201: Riesgo bajo. Esta vulnerabilidad permite a un atacante remoto realizar ataques XSS, debido a una sanitización insuficiente de los datos ingresados por el usuario al editor.

CVE-2021-39202: Riesgo bajo. Esta vulnerabilidad permite a un atacante remoto realizar ataques XSS debido a una sanitización insuficiente de los datos ingresados por el usuario al editor de widgets.

CVE-2021-39203: Riesgo medio. Esta vulnerabilidad permite a un atacante remoto comprometer el sistema objetivo. La vulnerabilidad existe debido a un error en el block editor bajo ciertas circunstancias.

Productos Afectados

WordPress 5.0 a 5.8.1

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

<https://wordpress.org/news/category/releases/>

<https://wordpress.org/news/2021/09/wordpress-5-8-1-security-and-maintenance-release/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39201>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39202>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39203>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39200>