Alerta de seguridad cibernética	9VSA22-00642-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2022
Última revisión	19 de mayo 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 afectan a dos plugins ampliamente usados en sitios WordPress: Jupiter y Tatsu.

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

Vulnerabilidades

CVE-2022-1654
CVE-2021-25094

Impacto

Vulnerabilidades críticas

CVE-2022-1654: Vulnerabilidad de escalamiento de privilegios en los plugin Jupiter y Jupiter X Core.

CVE-2021-25094: Vulnerabilidad de ejecución remota de código en el plugin Tatsu Builder.

Productos afectados

Jupiter y Jupiter X Core.
Tatsu Builder.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.wordfence.com/blog/2022/05/critical-privilege-escalation-vulnerability-in-jupiter-and-jupiterx-premium-themes/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1654
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25094