Vulnerabilidad Zero Day en plugin de WordPress permitiría cargar malware en los sitios web

Vulnerabilidad de tipo Zero Day en el plugin Fancy Product Designer para WordPress, permitiría que atacantes carguen malware en sitios web que tengan instalados dicho plugin, para fines ilícitos.

WordPress es una aplicación muy popular que permite la creación y edición de páginas web y a nivel global el 40% de todos los sitios web son gestionados por WordPress. Existen muchos desarrollos de plugins para la aplicación WordPress que están enfocados en enriquecer las opciones tanto del diseñador de un sitio como el nivel de experiencia de un usuario.

El plugin Fancy Product Designer cuenta con filtros para ejecución de archivos maliciosos, sin embargo se ha verificado que ante la carga de archivos PHP configurados maliciosamente, el plugin permitiría la carga de archivos tipo malware que eventualmente comprometerían los sistemas de información en los que se encuentra los sitios web WordPress.

En consideración al alto riesgo contra la confidencialidad, integridad y disponibilidad de los sitios web WorPress que cuenten con el plugin Fancy Product Designer, el EcuCERT recomienda a su comunidad objetivo, tomar en consideración las siguientes recomendaciones.

1. Aplicar los parches de actualización y mecanismos de contención emitidos por el desarrollador.

2. Ejecutar aplicaciones con perfiles de usuarios con el menor privilegio posible.

3. Implementar mecanismos de control de tráfico enfocados en conexiones atípicas.

Referencias

WORDFENCE. 2021. Critical 0-day in Fancy Product Designer Under Active Attack. Disponible en https://www.wordfence.com/blog/2021/06/critical-0-day-in-fancy-product-designer-under-active-attack/

NVD.NIST.GOV. 2021. CVE-2021-24370 Detail. Disponible en https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24370

FANCY PRODUCT DESIGNER. 2021. Critical 0-day in Fancy Product Designer Under Active Attack. Disponible en https://support.fancyproductdesigner.com/support/discussions/topics/13000029838