Alerta de seguridad cibernética	9VSA21-00387-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Febrero de 2021
Última revisión	09 de Febrero 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 afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre vulnerabilidades críticas que afectan al plugin NextGen Gallery de WordPress.

Este informe incluye las medidas de mitigación, consistentes en instalar las actualizaciones de los productos afectados cuando estén disponibles.

Vulnerabilidades

CVE-2020-35942
CVE-2020-35943

Impacto

CVE-2020-35942 es la más seria de ambas vulnerabilidades. Se debe a una falla lógica en la función de seguridad “is_authorized_request” de NextGen Gallery, que permite a un atacante, si logra engañar a un administrador para que haga clic a un enlace, enviar solicitudes especialmente diseñadas y realizar varias acciones maliciosas.

CVE-2020-35943 es una vulnerabilidad similar, relativa a otra función de seguridad de NextGen Gallery, “validate_ajax_request”. El atacante podría engañar al administrador para que envíe una solicitud pidiendo subir un archivo de imagen, en el que es posible esconder un webshell u otro código ejecutable PHP.

Productos afectados

Plugin NextGen Gallery para WordPress.

Mitigación

Instalar las actualización NextGen Gallery 3.5.0. desde el sitio del proveedor.

Enlaces

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35942

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35943