Alerta de seguridad informática	9VSA20-00128-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de enero de 2020
Última revisión	27 de enero de 2020

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, comparte la información referente a una vulnerabilidad detectada en el plug-in de Wordpress WPS Hide Login, complemento popular utilizado para ocultar la página de inicio de sesión predeterminada de WordPress (wp-login.php).

Vulnerabilidad

En la función plugins_loaded, el complemento busca diferentes subcadenas en la variable de entorno REQUEST_URI utilizando la función strpos, y debido a que algunos REQUEST_URI no se decodifican con la función rawurldecode, un atacante podría codificar esas subcadenas en la URL para evadir la detección, provocando que complemento redirigiría al usuario a la página de inicio de sesión oculta.

Productos Afectados

WPS Hide Login, versión 1.5.4.2 o inferior.

Mitigación

Actualizar WPS Hide Login a la versión 1.5.5

Enlace

https://wpvulndb.com/vulnerabilities/10046/
https://blog.nintechnet.com/wordpress-wps-hide-login-fixed-security-issue/