Alerta de seguridad informática	9VSA-00106-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Diciembre de 2019
Última revisión	21 de Diciembre de 2019

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 información obtenida de múltiples fuentes referente a vulnerabilidades que afectan al plugin '301 Redirects - Easy Redirect Manager' para WordPress. Este reporte incluye la respectiva mitigación.

Vulnerabilidad

CVE-2019-19915

Impactos

Redirección maliciosa, XSS y CSRF.
Esta vulnerabilidad permite a un atacante modificar la URL al que un sitio debiese redirigir al usuario. También permite la realización de ataques cross-site scripting (XSS) y cross-site request forgery (CSRF), esto debido a que las acciones AJAX, específicamente la función is_admin(), no validan correctamente qué usuario está modificando los valores de redirección, por lo que cualquier usuario registrado podría insertar URLs de publicidad o maliciosas.
También es posible gatillar un XSS reflejado, ya que el parámetro ID no sanitiza correctamente los datos ingresados por los usuarios.
Por último, un atacante también podría realizar ataques CSRF debido a la débil validación de usuario de las acciones AJAX.
Es urgente realizar la actualización de este plugin, pues la suma de estas 3 fallas podría resultar crítica para la víctima, arriesgando robo de credenciales, instalación de malware, robo de cookies, utilización de sus cuentas sin autorización, entre otros.

Producto Afectado

Desde la versión 1.1 hasta la versión 2.4 del plugin '301 Redirects - Easy Redirect Manager'

Mitigación

Actualizar a la versión 2.45 del plugin.

Enlaces

https://www.wordfence.com/blog/2019/12/critical-vulnerability-patched-in-301-redirects-easy-redirect-manager/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19915

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.12.21 15:34:12 -03'00'