BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-53
Fecha de publicación: 15/10/2024
Tema: Vulnerabilidad crítica en Jetpack
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Jetpack versiones :
  13.9.1, 13.8.2, 13.7.1, 13.6.1, 13.5.1, 13.4.4, 13.3.2, 13.2.3, 13.1.4, 13.0.1, 12.9.4, 12.8.2, 12.7. 2, 12.6.3, 12.5.1, 12.4.1, 12.3.1, 12.2.2, 12.1.2, 12.0.2, 11.9.3, 11.8.6, 11.7.3, 11.6.2, 11.5.3, 11.4.2, 11.3.4, 11.2.2, 11.1.4, 11.0.2, 10.9.3, 10.8.2, 10.7.2, 10.6.2, 10.5.3, 10.4.2, 10.3.2, 10.2.3, 10.1.2, 10.0.2, 9.9.3, 9.8.3, 9.7. 3, 9.6.4, 9.5.5, 9.4.4, 9.3.5, 9.2.4, 9.1.3, 9.0.5, 8.9.4, 8.8.5, 8.7.4, 8.6.4, 8.5.3, 8.4.5, 8.3.3, 8.2.6, 8.1.4, 8.0.3, 7.9.4, 7.8.4, 7.7.6, 7.6.4, 7.5.7, 7.4.5, 7.3.5, 7.2.5, 7.1.5, 7.0.5, 6.9.4, 6.8.5, 6.7.4, 6.6.5, 6.5.4, 6.4. 6, 6.3.7, 6.2.5, 6.1.5, 6.0.4, 5.9.4, 5.8.4, 5.7.5, 5.6.5, 5.5.5, 5.4.4, 5.3.4, 5.2.5, 5.1.4, 5.0.3, 4.9.3, 4.8.5, 4.7.4, 4.6.3, 4.5.3, 4.4.5, 4.3.5, 4.2.5, 4.1.4, 4.0.7, 3.9.10.

Descripción

El complemento Jetpack de WordPress lanzó una actualización de seguridad crítica para resolver una vulnerabilidad que permitía a los usuarios autenticados acceder a formularios enviados por otros visitantes.

Jetpack, desarrollado por Automattic, es un complemento popular que mejora la funcionalidad, seguridad y rendimiento de los sitios web en WordPress. Durante una auditoría de seguridad interna, se detectó una vulnerabilidad en la función de formulario de contacto de Jetpack desde la versión 3.9.9 (lanzada en 2016), que podría haber permitido a cualquier usuario con una sesión iniciada leer los formularios de otros visitantes.

Aunque no hay evidencia de que esta vulnerabilidad haya sido explotada, ahora que se ha lanzado la actualización, existe el riesgo de que alguien intente aprovecharla. Para mitigar el impacto, Jetpack trabajó con el equipo de complementos de WordPress.org para publicar parches en todas las versiones desde la 3.9.9. En caso de tener activas las actualizaciones automáticas de plugins, éste se actualizará automáticamente y no será necesaria ninguna

acción adicional. Sin embargo, si no lo tiene activo, deberá actualizarlo manualmente. En ambos casos se recomienda revisar la versión para asegurar que la actualización haya sido exitosa.

Solución

Se recomienda actualizar a la versión 13.9.1 de Jetpack para eliminar la falla. No se ha publicado soluciones alternativas ni mitigaciones para esta vulnerabilidad. Asegúrese de aplicar esta actualización lo antes posible para garantizar la seguridad de su sitio.

Información adicional:

- https://jetpack.com/blog/jetpack-13-9-1-critical-security-update/
- https://www.bleepingcomputer.com/news/security/jetpack-fixes-critical-information-disclosure-flaw-existing-since-2016/
- https://thehackernews.com/2024/10/wordpress-plugin-jetpack-patches-major.html

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com