
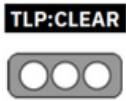


Nro. Alerta:	AL-2023-021	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 ALERTAS DE SEGURIDAD
TLP:			
Fecha:	01-jun-2023	Los piratas informáticos apuntan a 1,5 millones de sitios de WordPress con la explotación del complemento de consentimiento de cookies	Pág.: 1 of 5

I. DATOS GENERALES:

Clase de alerta: Incidente
Tipo de incidente: Compromiso de Aplicación
Nivel de riesgo: Alto

II. ALERTA


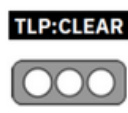
Los ataques en curso están dirigidos a una vulnerabilidad de secuencias de comandos entre sitios almacenados (XSS) no autenticadas en un complemento de consentimiento de cookies de WordPress llamado Beautiful Cookie Consent Banner con más de 40,000 instalaciones activas.



Figura 1.- Ilustraciones distintivas de Alerta Wordpress
 Fuente: BleepingComputer

III. INTRODUCCIÓN

En los ataques XSS, los actores de amenazas inyectan scripts JavaScript maliciosos en sitios web vulnerables que se ejecutarán dentro de los navegadores web de los visitantes.

Nro. Alerta:	AL-2023-021	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 ALERTAS DE SEGURIDAD
TLP:			
Fecha:	01-jun-2023	Los piratas informáticos apuntan a 1,5 millones de sitios de WordPress con la explotación del complemento de consentimiento de cookies	Pág.: 2 of 5

El impacto puede incluir acceso no autorizado a información confidencial, secuestro de sesiones, infecciones de malware a través de un redireccionamiento a sitios web maliciosos o un compromiso total del sistema del objetivo.

La empresa de seguridad de WordPress Defiant, que detectó los ataques, dice que la vulnerabilidad en cuestión también permite a los atacantes no autenticados crear cuentas de administrador no autorizadas en sitios web de WordPress que ejecutan versiones de complementos sin parches (hasta 2.10.1 inclusive).

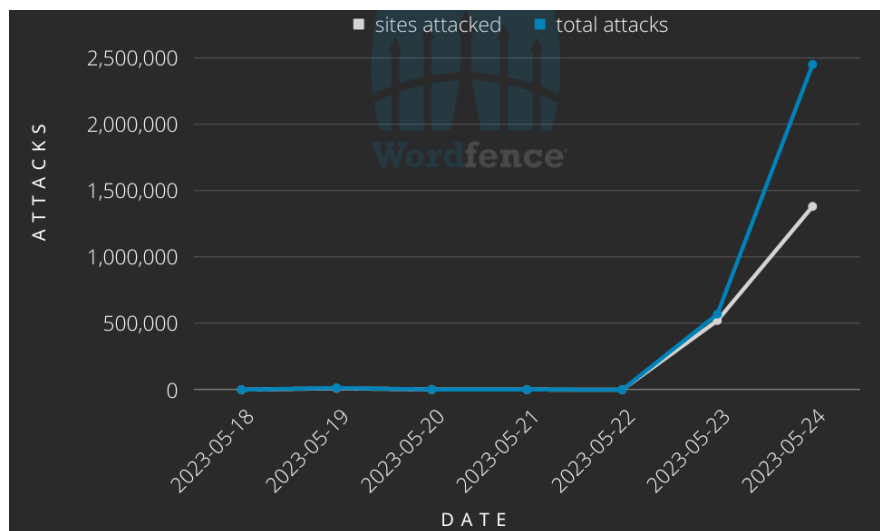

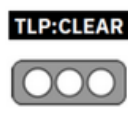


Figura 2.- Ataques Bloqueados (Wordfence)
 Fuente: BleepingComputer

A pesar de la naturaleza a gran escala de esta campaña de ataque en curso, el actor de amenazas utiliza un “exploit” mal configurado que probablemente no implementaría una carga útil incluso cuando se dirige a un sitio de WordPress que ejecuta una versión de complemento vulnerable.

Aun así, se recomienda a los administradores o propietarios de sitios web que utilizan el complemento Beautiful Cookie Consent Banner que lo actualicen a la última versión porque incluso un ataque fallido podría dañar la configuración del complemento almacenada en la opción: `nsc_bar_bannersettings_json`.

Nro. Alerta:	AL-2023-021	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	 V 1.1
TLP:			
Fecha:	01-jun-2023	Los piratas informáticos apuntan a 1,5 millones de sitios de WordPress con la explotación del complemento de consentimiento de cookies	Pág.: 3 of 5

Las versiones parcheadas del complemento también se han actualizado para repararse en caso de que el sitio web sea el objetivo de estos ataques.

Si bien es posible que la ola actual de ataques no pueda inyectar sitios web con una carga maliciosa, el actor de amenazas detrás de esta campaña podría abordar este problema en cualquier momento e infectar potencialmente cualquier sitio que permanezca expuesto.

La semana pasada, los actores de amenazas también comenzaron a investigar en Internet en busca de sitios web de WordPress que ejecutan versiones vulnerables de los complementos: Essential Addons para Elementor y WordPress Advanced Custom Fields.

Las campañas comenzaron después del lanzamiento de los exploits de prueba de concepto (PoC), que permitieron a los atacantes no autenticados secuestrar sitios web después de restablecer las contraseñas de administrador y obtener acceso privilegiado, respectivamente.

IV. VECTOR DE ATAQUE:

Las versiones 2.10.1 e inferiores de WordPress Beautiful Cookie Consent Banner sufren una vulnerabilidad de secuencias de comandos entre sitios persistentes no autenticadas. Explotar archivos ≈ Packet Storm


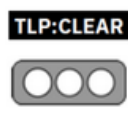
V. IMPACTO:

El impacto puede incluir acceso no autorizado a información confidencial, secuestro de sesiones, infecciones de malware a través de un redireccionamiento a sitios web maliciosos o un compromiso total del sistema del objetivo.

VI. INDICADORES DE COMPROMISO

La falla de seguridad explotada en esta campaña fue reparada en enero con el lanzamiento de la versión 2.10.2.

Se han bloqueado casi 3 millones de ataques contra más de 1,5 millones de sitios, desde casi 14000 direcciones IP desde el 23 de mayo de 2023.

Nro. Alerta:	AL-2023-021	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 ALERTAS DE SEGURIDAD
TLP:			
Fecha:	01-jun-2023	Los piratas informáticos apuntan a 1,5 millones de sitios de WordPress con la explotación del complemento de consentimiento de cookies	
		Pág.: 4 of 5	

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Actualizar complementos existentes. Si usa WordPress, puede verificar si tiene algún complemento que deba actualizarse iniciando sesión en su sitio y yendo a Panel de control > Actualizaciones. (Los elementos del menú Temas y complementos también tendrán círculos rojos junto a ellos si es necesario actualizarlos). Actualice todo.
- Active las actualizaciones automáticas para complementos. De forma predeterminada, WordPress no actualiza los complementos automáticamente. Puede habilitar esto por complemento yendo a la pantalla Complementos y haciendo clic en Habilitar actualizaciones automáticas junto a cada complemento.
- Eliminar complementos no compatibles. Vaya a la pantalla Complementos y haga clic en Ver detalles para cada complemento. Esta pantalla le muestra la última versión de WordPress con la que se probó el complemento y cuándo se actualizó por última vez. También mostrará una alerta si cree que el complemento ya no es compatible.
- Eliminar complementos innecesarios. Compruebe cuántos complementos y temas ha instalado en su sitio, menos es mejor.

VIII. DESCARGO DE RESPONSABILIDAD


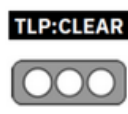
La información en la presente alerta; se proporciona con fines informativos.

Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.

La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

<https://www.bleepingcomputer.com/news/security/hackers-target-vulnerable-wordpress-elementor-plugin-after-poc-released/>

Nro. Alerta:	AL-2023-021	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	
TLP:			V 1.1
Fecha:	01-jun-2023	Los piratas informáticos apuntan a 1,5 millones de sitios de WordPress con la explotación del complemento de consentimiento de cookies	Pág.: 5 of 5

<https://www.bleepingcomputer.com/news/security/hackers-target-wordpress-plugin-flaw-after-poc-exploit-released/>

<https://www.bleepingcomputer.com/news/security/wordpress-custom-field-plugin-bug-exposes-over-1m-sites-to-xss-attacks/>

<https://cyberlegion.io/wordpress-beautiful-cookie-consent-banner-2-10-1-cross-site-scripting/>

<https://www.malwarebytes.com/blog/news/2023/05/beautiful-cookie-consent-banner-wordpress-plugin-vulnerability-update-now>

<https://wordpress.org/plugins/beautiful-and-responsive-cookie-consent/>