Actores maliciosos están explotando activamente una vulnerabilidad crítica en el tema de WordPress Service Finder, que permite obtener acceso no autorizado a cualquier cuenta del sitio, incluyendo cuentas de administrador, y tomar control total de las páginas afectadas.

Esta falla de seguridad, identificada como CVE-2025-5947 y con una puntuación CVSS de 9.8, impacta el complemento Service Finder Bookings, que viene incluido con el tema. La vulnerabilidad fue descubierta por un investigador conocido bajo el seudónimo *Foxyyy*.

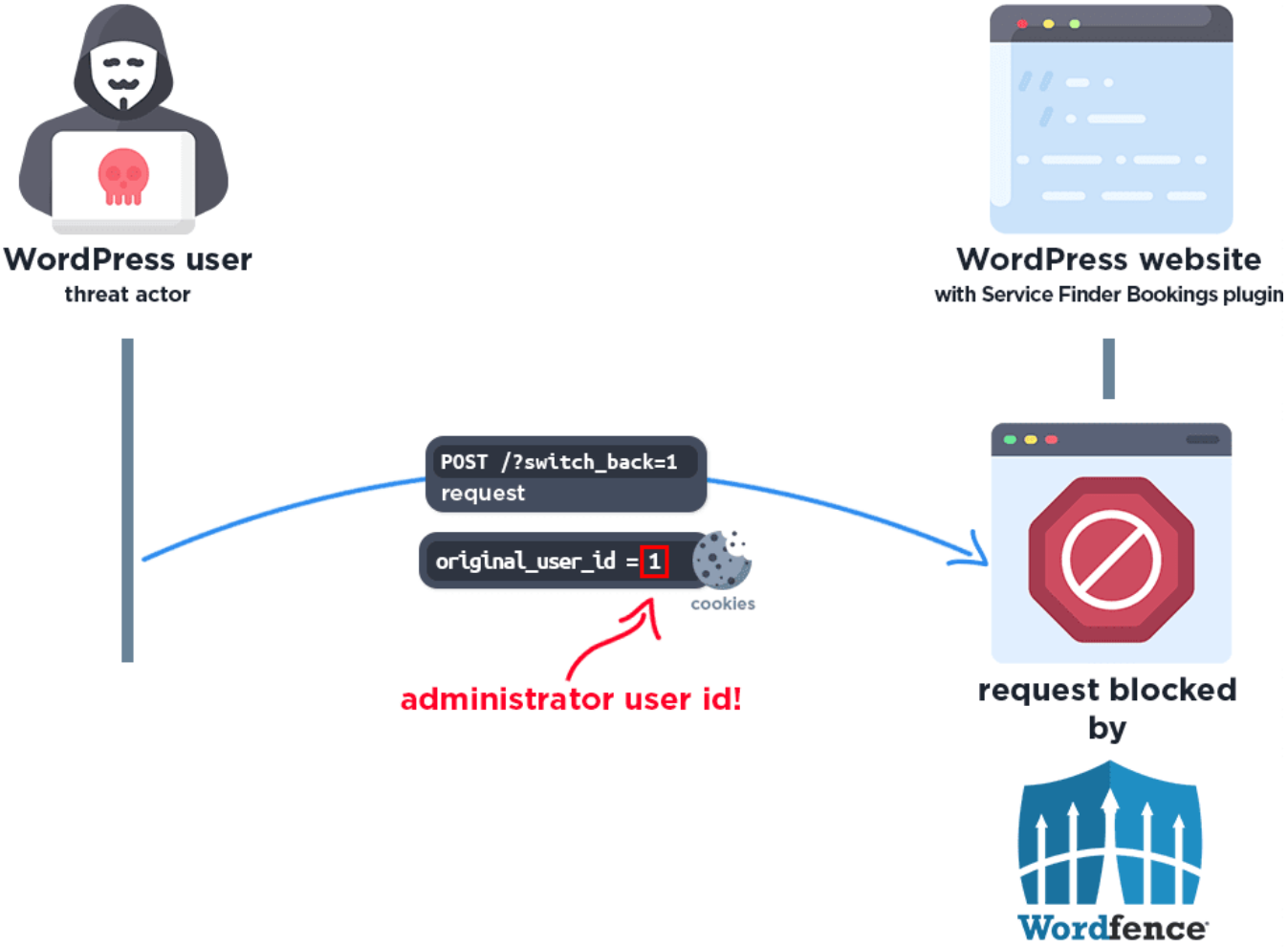
"Esta vulnerabilidad permite que un atacante no autenticado acceda a cualquier cuenta en el sitio, incluso aquellas con rol de 'administrador'", explicó el investigador de Wordfence *István Márton*.

El problema principal radica en una escalada de privilegios causada por un error en el proceso de autenticación. El complemento no valida adecuadamente el valor de las cookies del usuario antes de permitir el inicio de sesión mediante una función para cambiar de cuenta llamada `service_finder_switch_back()`.

Esto significa que un atacante externo, sin necesidad de credenciales válidas, puede explotar esta debilidad para iniciar sesión como cualquier usuario, incluyendo administradores, y así tomar control total del sitio web. A partir de ahí, podría insertar código malicioso, redirigir a los visitantes a sitios fraudulentos o incluso utilizar la página como plataforma para distribuir malware.

Esta vulnerabilidad afecta todas las versiones del tema hasta la 6.0 inclusive. El problema fue corregido por los desarrolladores del complemento el 17 de julio de 2025, con la publicación de la versión 6.1. Según datos del marketplace de Envato, el tema ha sido adquirido por más de 6,100 usuarios.

Desde el 1 de agosto de 2025, la empresa de seguridad WordPress ha detectado actividad de explotación dirigida a esta vulnerabilidad, registrando más de 13,800 intentos hasta la fecha. Sin embargo, aún no se ha determinado cuántos de estos intentos han sido exitosos.



Las siguientes direcciones IP han sido identificadas como responsables de ataques dirigidos a la función de cambio de cuentas del complemento Service Finder Bookings:

- 5.189.221.98
- 185.109.21.157
- 192.121.16.196
- 194.68.32.71
- 178.125.204.198

Se recomienda a los administradores de sitios revisar cuidadosamente sus páginas en busca

de comportamientos sospechosos y asegurarse de que todos los temas y complementos estén actualizados a su versión más reciente.