Si utilizas «*Ultimate Addons for Beaver Builder*» o «*Ultimate Addons for Elementor*», en tu sitio web con WordPress, podrías ser víctima de hackers.

Investigadores de seguridad descubrieron una vulnerabilidad de omisión de autenticación crítica pero fácil de explotar en ambos complementos premium de WordPress utilizados ampliamente, que podría permitir a los hackers remotos obtener acceso administrativo a los sitios sin requerir contraseñas.

Lo más preocupante es que los atacantes oportunistas ya comenzaron a explotar la vulnerabilidad en la naturaleza a solo 2 días del descubrimiento, para comprometer los sitios web vulnerables e instalar una puerta trasera maliciosa para un acceso posterior.

Los dos complementos vulnerables, creados por la compañía de desarrollo de software, Brainstorm Force, actualmente están impulsando cientos de miles de sitios web de WordPress utilizando los marcos de Elementor y Beaver Builder, ayudando a los administradores y diseñadores de sitios web a ampliar la funcionalidad de sus sitios con más widgets, módulos y plantillas de página.

Descubierto por investigadores del servicio de seguridad web MalCare, la vulnerabilidad reside en la forma en que ambos complementos permiten a los titulares de cuentas de WordPress, incluidos los administradores, autenticarse a través de los mecanismos de inicio de sesión de Facebook y Google.

Según el aviso de vulnerabilidad, debido a la falta de controles en el método de autenticación cuando un usuario inicia sesión por medio de Facebook o Google, los complementos vulnerables pueden ser engañados para permitir que usuarios malintencionados inicien sesión como cualquier otro usuario objetivo sin requerir ninguna contraseña.

> *«Sin embargo, los métodos de autenticación de Facebook y Google no verificaron el token devuelto por Facebook y Google, y dado que no requieren una contraseña, no hubo verificación de contraseña»*, explicaron los investigadores de WebARX, que

> también analizaron la falla y confirmaron que está activa.
>
> *«Para explotar la vulnerabilidad, el hacker necesita usar la identificación de correo electrónico de un usuario administrador del sitio. En la mayoría de los casos, esta información se puede recuperar con bastante facilidad»,* dijo MalCare.

WebARX confirmó a THN que los atacantes están abusando de esta falla para instalar un complemento falso de estadísticas de SEO luego de cargar un archivo tmp.zip en el servidor de WordPress objetivo, que finalmente deja caer un archivo de puerta trasera wp-xmlrpc.php a la raíz del directorio del sitio vulnerable.

MalCare descubrió esta vulnerabilidad el miércoles, que afecta a las versiones de los complementos que se enumeran a continuación y lo informó a los desarrolladores ese mismo día, mismos que luego abordaron rápidamente el problema y lanzaron versiones parcheadas de ambos en solo 7 horas.

- Complementos definitivos para Elementor <= 1.20.0
- Complementos definitivos para Beaver Builder <= 1.24.0

La vulnerabilidad de omisión de autenticación se ha parcheado con el lanzamiento de *«Ultimate Addons for Elementor 1.20.1» y «Ultimate Addons for Beaver Builder 1.24.1»*, que se recomienda instalar lo más pronto posible.