Un investigador de seguridad cibernética reveló hoy de forma pública, los detalles y código de explotación de prueba de concepto, para una vulnerabilidad crítica de ejecución remota de código de día cero sin parches, que afecta al software de foros de Internet, vBulletin, y que se encuentra bajo explotación activa en la naturaleza.

vBulletin es un paquete de software de foro de Internet patentado, ampliamente utilizado basado en PHP y MySQL, utilizado actualmente por más de 100 mil sitios web en Internet, incluyendo sitios dentro del Top 1 millón de Alexa y Fortune 500.

En septiembre del año pasado, un investigador de seguridad anónimo separado, reveló públicamente una vulnerabilidad RCE de día cero en vBulletin, identificada como CVE-2019-16759, y recibió una calificación de gravedad crítica de 9.8, lo que permite a los atacantes ejecutar comandos maliciosos en el servidor remoto sin necesidad de autenticación para iniciar sesión en el foro.

Un día después de la divulgación de dicha vulnerabilidad, el equipo de vBulletin lanzó parches de seguridad para resolver el problema, pero el parche fue insuficiente para bloquear la explotación de la falla.

La nueva vulnerabilidad 0-day, descubierta y publicada por el investigador Amir Etemadieh (Zenofex), es un bypass para CVE-2019-16759. La falla no ha recibido ningún identificador CVE hasta ahora.

Esta última vulnerabilidad de día cero debe considerarse como un problema grave, ya que se puede explotar de forma remota y no requiere autenticación. Se puede explotar fácilmente utilizando un código de explotación de un solo comando en una línea que puede resultar en la ejecución remota de código en el último software vBulletin.

Según el investigador, el parche para CVE-2019-16759, no resolvió los problemas presentes en la plantilla *«widget_tabbedcontainer_tab_panel»*, es decir, su capacidad para cargar una plantilla secundaria controlada por el usuario, tomar un valor de otro nombrado por separado y colocarlo en una variable llamada *«widgetConfig»*, lo que efectivamente permite al

investigador omitir el parche para CVE-2019-16759.

El investigador también publicó tres cargas útiles de exploits de prueba de concepto escritas en varios idiomas, incluidos Bash, Python y Ruby.

Explotación activa de la vulnerabilidad de día cero

Poco después del lanzamiento del código de explotación PoC, los hackers comenzaron a explotar la vulnerabilidad para apuntar a foros de vBulletin.

Según Jeff Moss, creador de las conferencias de seguridad de DefCon y BlackHat, el foro de DefCon también fue atacado con el exploit solo 3 horas después de que se revelara la falla.

> *«Un nuevo Zero Day para vBulletin fue lanzado ayer por @Zenofex que reveló que el parche CVE-2019-16759 estaba incompleto, en tres horas, forum.defcon.org fue atacado, pero estábamos listos para ello. Desactive la representación PHP y ¡protégase hasta que lo reparen!»,* dijo Moss.

Mientras tanto, el equipo de vBulletin respondió inmediatamente a la falla publicada y lanzó un nuevo parche de seguridad que deshabilita el módulo PHP en el software vBulletin para solucionar el problema, asegurando a sus usuarios que se eliminará por completo en la próxima versión de vBulletin, la 5.6.4.

Los mantenedores del software aconsejaron a los desarrolladores que consideren vulnerables todas las versiones anteriores de vBulletin y actualicen sus sitios para ejecutar vBulletin 5.6.2 lo antes posible. Los desarrolladores pueden consultar la descripción general rápida: Actualización de vBulletin Connect en los foros de soporte para más información.

En caso de no poder actualizar inmediatamente el software, como forma de mitigación se recomienda desactivar los widgets PHP dentro de los foros de la siguiente forma:

Acceder al panel del administrador de vBulletin y hacer clic en *«Configuración»* en el menú de la izquierda, luego en *«Opciones»* en el menú desplegable.

Elegir *«Configuración general»* y luego hacer clic en *«Editar configuración».*

Buscar *«Deshabilitar PHP, HTML estático y la representación del módulo de anuncios»,* establecer en *«Sí»* y dar clic en guardar.

Aunque estos cambios podrían romper algunas funciones, servirán como mitigación del problema hasta que se apliquen los parches.