Un pirata informático anónimo reveló hoy públicamente detalles y código de explotación de prueba de concepto para una vulnerabilidad de ejecución remota de código de día cero sin parches en vBulletin, uno de los software de foros de Internet más utilizados.

Una de las razones por las cuales la vulnerabilidad debe verse como un problema grave no es solo porque es explotable de forma remota, sino que tampoco requiere autenticación.

Escrito en PHP, vBulletin es un paquete de software de foro de Internet patentado ampliamente utilizado, que impulsa más de 100 mil sitios web en Internet, incluyendo el top 1 millón de sitios web y foros de empresas en Fortune 500 y Alexa.

Según los detalles publicados en la lista de correo de Full Disclosure, el pirata informático afirma haber encontrado una vulnerabilidad de ejecución remota de código que parece afectar las versiones de vBulletin 5.0.0 hasta la última 5.5.4.

La vulnerabilidad reside en la forma en que un archivo de widget interno del paquete de software del foro acepta configuraciones a través de los parámetros de URL y luego las analiza en el servidor sin las comprobaciones de seguridad adecuadas, lo que permite a los atacantes inyectar comandos y ejecutar código de forma remota en el sistema.

Como prueba de concepto, el pirata informático también ha lanzado un exploit basado en python que podría facilitar que cualquiera explote el día cero en la naturaleza.

Hasta ahora, el número de vulnerabilidades y exposiciones comunes (CVE) no se ha asignado a esta vulnerabilidad.

The Hacker News informó también a los responsables del proyecto vBulletin acerca de la divulgación de la vulnerabilidad y espera que corrijan el problema de seguridad antes de que los hackers comiencen a explotarlo para apuntar a las instalaciones de vBulletin.

Un investigador independiente de seguridad cibernética analizó la razón principal de esta vulnerabilidad y publicó detalles.

Mientras tanto, un usuario de GitHub también lanzó un script simple que podría permitir a cualquier persona escanear Internet para encontrar sitios web de vBulletin usando el motor de búsqueda Shodan y buscar de forma automática sitios vulnerables.