Los desarrolladores del proyecto vBulletin anunciaron recientemente una actualización importante para corregir una vulnerabilidad, aunque no revelaron ninguna información técnica sobre ésta, identificada como CVE-2020-12720.

Escrito en PHP, vBulletin es un software de foro de Internet ampliamente utilizado que impulsa más de 100 mil sitios web en Internet, incluyendo los foros para algunas compañías como Fotune 500.

Teniendo en cuenta que el popular software de foro también es uno de los objetivos favoritos de los hackers, retener los detalles de la vulnerabilidad podría ayudar a muchos sitios web a aplicar parches antes de que los piratas informáticos puedan explotarla y comprometer sitios web, servidores y sus bases de datos.

Sin embargo, al igual que en otras ocasiones, los investigadores y los hackers ya comenzaron a realizar ingeniería inversa del parche de software para localizar y comprender la vulnerabilidad.

National Vulnerability Database (NVD), también se encuentra analizando la falla y reveló que se originó por un problema de control de acceso incorrecto que afecta vBulletin antes de 5.5.6pl1, 5.6.0.

> *«Si está utilizando una versión de vBulletin 5 Connect anterior a 5.5.2, es imprescindible actualizar lo antes posible»*, dijo vBulletin.

Aunque no había un código de prueba de concepto disponible hasta el momento, se espera que un exploit para la vulnerabilidad no tarde mucho en aparecer en línea.

Charles Fol, un ingeniero de seguridad en Ambionics, confirmó que descubrió e informó responsablemente esta vulnerabilidad al equipo de vBulletin, y tiene planes de divulgar más información durante la conferencia SSTIC que está programada para el siguiente mes.

Se recomienda a los administradores del foro que descarguen e instalen los parches respectivos para las siguientes versiones del software de foro lo antes posible.