Después de lanzar un parche para una vulnerabilidad crítica de día cero, de ejecución remota de código a fines del mes pasado, vBulletin publicó recientemente una nueva actualización de parche de seguridad que aborda 3 vulnerabilidades más de alta gravedad en su software de foro.

Si no se repara, las vulnerabilidades de seguridad reportadas, que afectan el vBulletin 5.5.4 y versiones anteriores, eventualmente podrían permitir a los atacantes remotos tomar el control completo sobre los servidores web específicos y robar información confidencial del usuario.

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, incluidos Fortune 500 y Alexa.

Descubierta por el investigador de seguridad de aplicaciones Egidio Romano, la primera vulnerabilidad, rastreada como CVE-2019-17132, es una falla de ejecución remota de código, mientras que las otras dos son problemas de inyección de SQL, a ambas se les asignó una única identificación como CVE-2019-17271.

Vulnerabilidades RCE y SQLi

La falla de RCE reside en la forma en que el foro vBulletin maneja las solicitudes de los usuarios para actualizar los avatares de sus perfiles, un icono o una representación gráfica del usuario, lo que permite a un atacante remoto inyectar y ejecutar código PHP arbitrario en el servidor de destino por medio de parámetros no autorizados.

Sin embargo, debe tenerse en cuenta que esta vulnerabilidad no es explotable en la instalación predeterminada del foro vBulletin, sino que es posible la explotación cuando el administrador del sitio web habilita la opción *«Guardar avatares como archivos».* Romano lanzó un exploit público de prueba de concepto para esta vulnerabilidad.

Las otras dos vulnerabilidades son problemas de inyección SQL en banda y basados en

tiempo, que residen en dos puntos finales separados y podrían permitir a los administradores con privilegios restringidos leer datos confidenciales de la base de datos, a los que de otra forma no se les permitiría acceder.

Ya que estos dos defectos de inyección SQL no pueden ser explotados por ningún usuario registrado y requieren permisos especiales, los administradores y usuarios del foro vBulletin no deben entrar en pánico.

Romano informó responsablemente todas las vulnerabilidades a los encargados del proyecto vBulletin la semana pasada, el 30 de septiembre, y el equipo reconoció sus hallazgos y lanzó las siguientes actualizaciones de parches de seguridad que abordan los defectos reportados.

- vBulletin 5.5.4 Patch Level 2
- vBulletin 5.5.3 Patch Level 2
- vBulletin 5.5.2 Patch Level 2

Se recomienda a los administradores que apliquen el parche de seguridad antes de que los hackers comiencen a explotar las vulnerabilidades para apuntar a los usuarios de su foro, tal como ya ocurrió la semana pasada, donde el atacante robó información de inicio de sesión de 245 mil usuarios de los Foros de Comodo, luego de que la compañía no pudo aplicar los parches a tiempo.