Investigadores de seguridad cibernética revelaron el viernes una vulnerabilidad crítica ya parcheada en múltiples versiones de un popular sistema de facturación y tiempo llamado BillQuick, que está siendo explotado activamente por los atacantes para implementar ransomware en sistemas vulnerables.

CVE-2021-42258 se refiere a un ataque de inyección basado en SQL que permite la ejecución remota de código y se aprovechó con éxito para obtener acceso inicial a una empresa de ingeniería estadounidense anónima y montar un ataque de ransomware, dijo la compañía estadounidense de ciberseguridad, Huntress Labs.

Aunque el problema fue abordado por BQE Software en la versión 22.0.9.1 de BillQuick lanzada el 7 de octubre, otros ocho problemas de seguridad no revelados que se identificaron como parte de la investigación aún no se han solucionado. Según su sitio web, los productos de BQE Software son utilizados por unos 400 mil usuarios en todo el mundo.

> *«Los hackers pueden usar esto para acceder a los datos BillQuick de los clientes y ejecutar comandos maliciosos en sus servidores Windows locales. Este incidente pone de relieve un patrón repetido que afecta al software para pymes: los proveedores bien establecidos están haciendo muy poco para proteger de forma proactiva sus aplicaciones y someten a sus clientes involuntarios a una responsabilidad significativa cuando los datos confidenciales se filtran o rescatan de forma inevitable»*, dijo Caleb Stewart, investigador de amenazas de Huntress Labs.

Esencialmente, la vulnerabilidad proviene de cómo BillQuick Web Suite 2020 se construye de consultas de bases de datos SQL, lo que permite a los atacantes inyectar un SQL especialmente diseñado a través del formulario de inicio de sesión de la aplicación que podría usarse para generar de forma remota un shell de comandos en el sistema operativo Windows subyacente y lograr la ejecución del código, que a su vez, es posible por el hecho de que el software se ejecuta como usuario *«administrador del sistema».*

> *«Los hackers están constantemente buscando frutos a la mano y vulnerabilidades que pueden explotarse, y no siempre están hurgando en aplicaciones grandes como Office. A veces una herramienta de productividad o incluso un complemento puede ser la puerta por la que los hackers atraviesan para obtener acceso a un entorno y llevar a cabo su próximo movimiento»,* dijo Stewart.