Se ha observado que actores maliciosos están dirigiendo sus ataques al sector de la construcción mediante la infiltración en el software de contabilidad FOUNDATION, según recientes hallazgos de Huntress.

> *«Los atacantes han estado realizando ataques de fuerza bruta al software a gran escala, logrando acceder simplemente usando las credenciales predeterminadas del producto»*, señaló la empresa de ciberseguridad.

Las industrias afectadas por esta amenaza emergente incluyen plomería, HVAC (calefacción, ventilación y aire acondicionado), concreto, y otros subsectores relacionados.

El software FOUNDATION utiliza un servidor Microsoft SQL (MS SQL) para gestionar las operaciones de bases de datos y, en algunos casos, tiene el puerto TCP 4243 abierto, lo que permite el acceso directo a la base de datos a través de una aplicación móvil.

Según Huntress, el servidor contiene dos cuentas de alto privilegio: «sa», una cuenta de administrador del sistema por defecto, y «dba», una cuenta creada por FOUNDATION, que en muchos casos permanecen con las credenciales predeterminadas sin modificar.

Como consecuencia, los actores maliciosos podrían realizar ataques de fuerza bruta contra el servidor y aprovechar la opción xp_cmdshell para ejecutar comandos de shell arbitrarios.

> *«Este procedimiento almacenado extendido permite la ejecución de comandos del sistema operativo directamente desde SQL, lo que facilita a los usuarios ejecutar scripts y comandos de shell como si tuvieran acceso al símbolo del sistema del sistema operativo»,* explicó Huntress.

Los primeros indicios de esta actividad fueron detectados por Huntress el 14 de septiembre de 2024, tras registrar cerca de 35,000 intentos de inicio de sesión por fuerza bruta contra

un servidor MS SQL en un host, hasta lograr acceso exitoso.

De los 500 hosts que ejecutan el software FOUNDATION en los puntos protegidos por la empresa, 33 de ellos se encontraron accesibles públicamente con las credenciales predeterminadas.

Para reducir el riesgo de estos ataques, se recomienda cambiar las credenciales predeterminadas, evitar exponer la aplicación en Internet si es posible, y desactivar la opción xp_cmdshell cuando sea necesario.