Investigadores de Seguridad Cibernética encontraron vulnerabilidades críticas en dos populares sistemas industriales de acceso remoto que pueden explotarse para prohibir el acceso a plantas de producción industrial, piratear piratear redes de empresas, manipular datos e incluso robar secretos comerciales confidenciales.

Las vulnerabilidades, descubiertas por OTORIO, con sede en Tel Aviv, fueron identificadas en SiteManager y GateManager de B&R Automation y mbCONNECT24, de MB Connect Line, dos de las herramientas de mantenimiento remoto más populares utilizadas en los sectores de automoción, energía, petróleo y gas, metal y embalaje, para conectarse a activos industriales de cualquier parte del mundo.

Según un aviso publicado por la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA) el miércoles, la explotación exitosa de las vulnerabilidades de B&R Automation, podría permitir la *«divulgación arbitraria de información, manipulación y una condición de denegación de servicio».*

Las fallas, que van desde el cruce de la ruta hasta la autenticación incorrecta, afectan todas las versiones de SiteManager antes de la v9.2.620236042, GateManager 4260 y 9250 antes de la v9.0.20262 y GateManager 8250 antes de la v9.2.620236042.

Nikolay Sokolik y Hay Mizrachi de OTORIO, descubrieron que al explotar las seis vulnerabilidades (CVE-2020-11641 a CVE-2020-11646), un atacante autenticado con acceso a la solución a través de una licencia general, podría ver información confidencial sobre otros usuarios, sus activos, y sus procesos, aún cuando pertenezcan a una organización diferente a la del adversario.

> *«Los atacantes pueden utilizar esta información para apuntar a otras organizaciones y sus sistemas industriales»,* dijo OTORIO.

> *«Además, los hackers pueden engañar a los usuarios para que accedan a sitios extranjeros maliciosos a través de alertas y mensajes del sistema falsos. El atacante también puede activar un reinicio repetido tanto de GateManager como de SiteManager, lo que eventualmente provocará una pérdida de disponibilidad y la interrupción de la producción».*

De igual forma, las versiones de mymbCONNECT24 y mbCONNECT24 v2.6.1 y anteriores, se encontraron vulnerables a cuatro problemas de seguridad diferentes, que podría hacer posible que un atacante que haya iniciado sesión acceda a información arbitraria a través de la inyección de SQL, robe los detalles de la sesión mediante una solicitud entre sitios y realice ataque de falsificación (CSRF), simplemente con un enlace diseñado especialmente, y aproveche las bibliotecas de terceros obsoletas y no utilizadas incluidas con el software para obtener la ejecución remota de código.

La vulnerabilidad RCE es la más grave de todas, con una puntuación CVSS de 9.8 sobre 10.

Aunque las fallas se solucionaron desde entonces, el desarrollo demuestra cómo las debilidades en las soluciones de acceso remoto pueden tener consecuencias destructivas en la infraestructura crítica.

CISA por su parte, recomienda minimizar la exposición de la red para todos los dispositivos del sistema de control, además de poner las redes del sistema de control y los dispositivos remotos detrás de firewalls y aislarlos de la red empresarial.

> *«Cuando se requiera acceso remoto, utilice métodos seguros, como redes privadas virtuales (VPN), reconociendo que las VPN pueden tener vulnerabilidades y deben actualizarse a la versión más actual disponible»,* advirtió la agencia.