Una nueva investigación reveló lo que se denomina una vulnerabilidad de seguridad en Microsoft 365 que podría explotarse para inferir el contenido de los mensajes debido al uso de un algoritmo criptográfico roto.

> *«Los mensajes están encriptados en un modo de operación inseguro Electronic Codebook (ECB)»,* dijo la compañía finlandesa de seguridad cibernética WithSecure.

El cifrado de mensajes de Office 365 (OME) es un mecanismo de seguridad que se utiliza para enviar y recibir mensajes de correo electrónico cifrados entre usuarios dentro y fuera de una organización sin revelar nada sobre las comunicaciones en sí.

Una consecuencia del problema recientemente revelado es que los terceros deshonestos que obtienen acceso a los mensajes de correo electrónico cifrados pueden descifrar los mensajes, rompiendo efectivamente las protecciones de confidencialidad.

Electronic Codebook es uno de los modos más simples de cifrado en el que cada bloque de mensaje se codifica por separado mediante una clave, lo que significa que los bloques de texto sin formato idénticos se transpondrán en bloques de texto cifrado idénticos, lo que lo hace inadecuado como protocolo criptográfico.

El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST), dijo a inicios de este año que *«el modo ECB encripta bloques de texto sin formato de forma independiente, sin aleatorización; por lo tanto, la inspección de dos bloques de texto cifrado cualesquiera revela si los bloques de texto sin formato correspondientes son iguales o no».*

De este modo, le deficiencia identificada por WithSecure no se relaciona con el descifrado de un solo mensaje en sí, sino que se basa en analizar un alijo de correos robados encriptados en busca de patrones con fugas, y posteriormente, decodificar el contenido.

> *«Un atacante con una gran base de datos de mensajes puede inferir su contenido (o*

> *partes de él) analizando las ubicaciones relativas de las secciones repetidas de los mensajes interceptados»,* dijo la compañía.

Los hallazgos se suman a las crecientes preocupaciones de que la información cifrada previamente filtrada puede ser descifrada y explotada para ataques en el futuro, una amenaza llamada *«piratear ahora, descifrar más tarde»*, que alimenta la necesidad de cambiar algoritmos resistentes a la cuántica.

Microsoft, por su parte considera a OME como un sistema heredado, y la compañía recomienda a los clientes que usen una plataforma de gobierno de datos llamada Purview para proteger los correos electrónicos y los documentos a través del cifrado y los controles de acceso.

> *«Aunque ambas versiones pueden coexistir, le recomendamos encarecidamente que edite sus reglas de flujo de correo antiguas que usan la acción de regla Aplicar a la versión anterior de OME para usar Microsoft Pureview Message Encryption»*, dijo Redmond en su documentación.

> *«Debido a que Microsoft no tiene planes para solucionar esta vulnerabilidad, la única mitigación es evitar el uso de Microsoft Office 365 Message Encryption»,* dijo WithSecure.