Microsoft reveló el lunes que mitigó una vulnerabilidad de seguridad que afectaba a Azure Synapse y Azure Data Factory que, de ser explotada con éxito, podría resultar en la ejecución remota de código.

La vulnerabilidad, rastreada como CVE-2022-29972, fue denominada como «SynLapse» por investigadores de Orca Security, quienes informaron la vulnerabilidad a Microsoft en enero de 2022.

> *«La vulnerabilidad era específica del Controlador de Conectividad Abierta de Base de Datos (ODBC) de terceros que se utiliza para conectarse a Amazon Redshift en las canalizaciones de Azure Synapse y Azure Data Factory Integration Runtime (IR) y no afectó a Azyre Synapse en su totalidad»,* dijo la compañía.

> *«La vulnerabilidad podría haber permitido que un atacante realizara la ejecución de comandos remotos a través de la infraestructura IR sin limitarse a un solo inquilino».*

En otras palabras, un actor malintencionado puede armar el error para adquirir el certificado del servicio Azure Data Factory y acceder a Integration Runtimes de otro arrendatario para obtener acceso a información confidencial, rompiendo efectivamente las protecciones de separación de arrendatarios.

La compañía, que resolvió la falla de seguridad el 15 de abril, dijo que no encontró evidencia de uso indebido o actividad maliciosa asociada con la vulnerabilidad en la naturaleza.

Debido a esto, la compañía con sede en Redmond compartió las detecciones de Microsoft Defender para Endpoint y Microsoft Defender Antivirus, para proteger a los clientes de una posible explotación, y agregó que está trabajando para reforzar la seguridad de los conectores de datos de terceros al trabajar con proveedores de controladores.

Los hallazgos llegaron poco más de dos meses después de que Microsoft corrigiera una vulnerabilidad de *«AutoWarp»* que afectaba su servicio Azure Automation y que podría haber permitido el acceso no autorizado a otras cuentas de clientes de Azure y tomar el control.

El mes pasado, Microsoft también resolvió un par de problemas, denominados «ExtraReplica«, con Azure Database for PostgreSQL Flexible Server, que podrían dar lugar a un acceso no aprobado a la base de datos entre cuentas en una región.