Vulnerabilidad SynLapse

BCSC-VULNERABILIDAD-SYNLAPSE

TLP:WHITE

www.basquecybersecurity.eus

Mayo 2022

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Respuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

1. RESUMEN EJECUTIVO

El equipo de Microsoft ha hecho pública una vulnerabilidad que afecta a las canalizaciones de Azure Synapse y Azure Data Factory, y que podría permitir a un atacante ejecutar comandos remotos en la infraestructura de Integration Runtime (IR), dedicada a proporcionar funcionalidades de integración de datos en entornos de red.

La vulnerabilidad, catalogada con el identificador CVE-2022-29972 y denominada **SynLapse,** fue descubierta por el investigador Tzah Pahima y mitigada el 15 de abril, sin evidencia de explotación antes de que se publicaran las correcciones. Este fallo era específico del controlador de Conectividad abierta de base de datos (ODBC) de terceros que se usa para conectarse a Amazon Redshift en las canalizaciones de Azure Synapse y Azure Data Factory Integration Runtime (IR) por lo que no afectó a Azure Synapse en su totalidad.

Los atacantes pueden explotar esta vulnerabilidad para acceder y controlar los espacios de trabajo de Synapse de otros clientes, lo que les permitiría filtrar datos confidenciales, incluidas las claves de servicio de Azure, los tokens de API y las contraseñas de otros servicios.

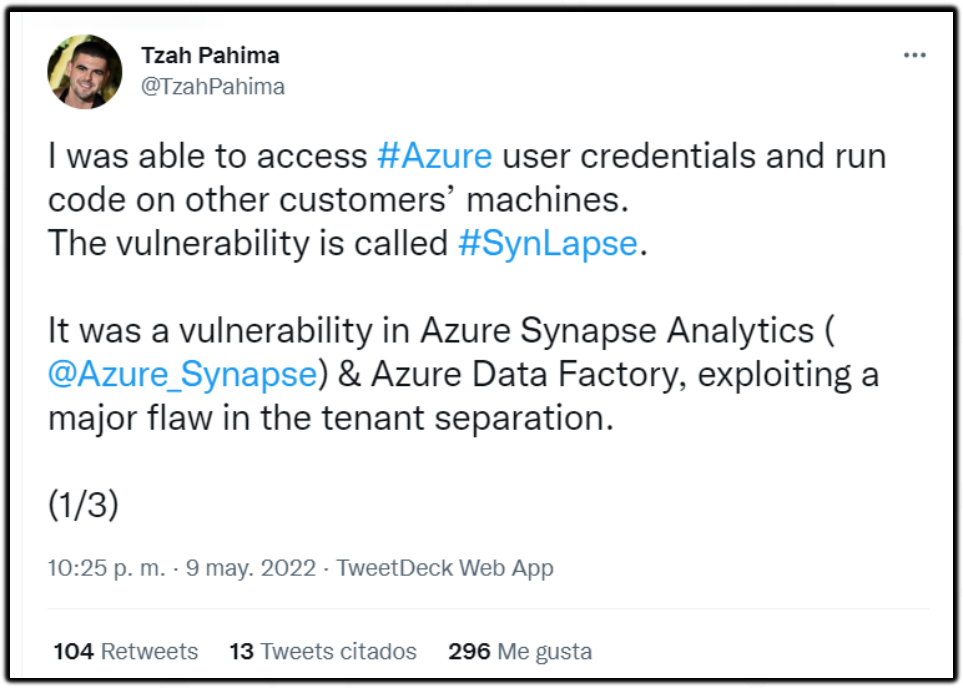

Imagen 1: Tweet del investigador Tzah Pahima alertando de la vulnerabilidad

2. ANÁLISIS TÉCNICO

Recientemente, analistas de ciberseguridad de la empresa especializada en seguridad en la nube, Orca Security, informaron sobre una vulnerabilidad crítica en Azure Synapse y Azure Data Factory, a la que catalogaron bajo el nombre SynLapse.

Esta vulnerabilidad, reportada el pasado 4 de enero por el especialista en ciberseguridad, Tzah Pahima, puede permitir a un atacante acceder y controlar los espacios de trabajo de Synapse de otros clientes y filtrar datos confidenciales almacenados en el servicio, incluidas las claves de servicio de Azure, los tokens de API y las contraseñas de otros servicios.

Desde Microsoft, el pasado 10 de abril, se informó que el problema se había solucionado, sin embargo, la solución aún era parcial y, en menos de 24 horas, el equipo de Orca Security consiguió otro vector de ataque que permitía eludir la separación de usuarios en este servicio para permitir el acceso a los datos de otros clientes.

Esta nueva vulnerabilidad, catalogada con el identificador CVE-2022-29972, aprovecha un error en la infraestructura informática de Integration Runtime (IR), utilizada por las canalizaciones de Azure Synapse y Azure Data Factory para proporcionar funcionalidades de integración de datos en entornos de red, por ejemplo, flujo de datos, distribución de actividades o ejecución de paquetes de SQL Server Integration Services (SSIS). La vulnerabilidad podría permitir a un atacante ejecutar código de forma remota en toda la infraestructura IR sin limitarse a un solo inquilino.

En una posible etapa de ataque posterior, es probable que se puedan robar los certificados de servicio de la unidad de fabricación de datos de Azure para ejecutar instrucciones en los tiempos de ejecución de integración de la unidad de fabricación de datos de Azure de otro inquilino.

3. MITIGACIÓN / SOLUCIÓN

Como es habitual, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

Por su lado, Microsoft afirma que todos los clientes que usan la nube de Azure (Azure Integration Runtime) o que alojan su propio entorno local (Self-Host (SHIR)), no necesitan realizar ninguna medida adicional, salvo aplicar las actualizaciones automáticas que ofrece el fabricante. Igualmente, los clientes con IR Self-Host (SHIR) que no tengan activada la actualización automática han sido contactados a través de Azure Service Health Alerts para que actualicen sus SHIR a la última versión disponible: 5.17.8154.2.

De manera adicional, Microsoft recomienda a los usuarios configurar los espacios de trabajo de Synapse con una red virtual administrada para conseguir un mejor aislamiento informático y de red.

Por último, de forma complementaria, se puede encontrar más información para mitigar de manera completa la vulnerabilidad **SynLapse,** en el apartado "Recomendaciones del cliente y soporte adicional" de la publicación del blog de Microsoft.

4. REFERENCIAS ADICIONALES

- Vulnerability mitigated in the third-party Data Connector used in Azure Synapse pipelines and Azure Data Factory (CVE-2022-29972).
- Security Advisory: Insufficient Tenant Separation in Azure Synapse Service.
- Integration runtime in Azure.
- NIST: CVE-2022-29972.
- Amazon Redshift.
- Orca security website.
- Azure Synapse Analytics.
- Azure Data Factory.
- Azure Synapse Analytics Managed Virtual Network.
- Tzah Pahima official twitter page.
- Microsoft Integration Runtime.
- Conectividad abierta de bases de datos (ODBC).
- Información general de Service Health.

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?