Home (https://www.bleepingcomputer.com/) › News (https://www.bleepingcomputer.com/news/) › Security (https://www.bleepingcomputer.com/news/security/) › Microsoft releases fixes for Azure flaw allowing RCE attacks

Microsoft releases fixes for Azure flaw allowing RCE attacks

By
Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)

May 9, 2022 01:42 PM **0**

Microsoft has released security updates to address a security flaw affecting Azure Synapse and Azure Data Factory pipelines that could let attackers execute remote commands across Integration Runtime infrastructure.

The Integration Runtime (IR) (https://docs.microsoft.com/en-us/azure/data-factory/concepts-integration-runtime) compute infrastructure is used by Azure Synapse and Azure Data Factory pipelines to provide data integration capabilities across network environments (e.g., data flow, activity dispatch, SQL Server Integration Services (SSIS) package execution).

The vulnerability (tracked as CVE-2022-29972 and dubbed **SynLapse (https://orca.security/resources/blog/azure-synapse-analytics-security-advisory/)** by Orca Security Tzah Pahima) was mitigated on April 15, with no evidence of exploitation before fixes were released.

(https://www.bleepingcomputer.com/news/security/hackers-display-blood-is-on-your-hands-on-russian-tv-take-down-rutube/?traffic_source=Connatix)

Hackers display “blood is on your hands" on Russian TV, take down RuTube

According to Pahima's findings, attackers can exploit this bug to access and control other customers' Synapse workspaces, allowing them to leak sensitive data including Azure's service keys, API tokens, and passwords to other services.

Tzah Pahima
@TzahPahima

I was able to access #Azure user credentials and run code on other customers’ machines. The vulnerability is called #SynLapse.

It was a vulnerability in Azure Synapse Analytics (@Azure_Synapse) & Azure Data Factory, exploiting a major flaw in the tenant separation.

(1/3)

4:25 AM · May 10, 2022

Read the full conversation on Twitter

"The vulnerability was found in the third-party ODBC data connector used to connect to Amazon Redshift, in Integration Runtime (IR) in Azure Synapse Pipelines, and Azure Data Factory," Microsoft explained (https://msrc.microsoft.com/update-guide/vulnerability/ADV220001) in a security advisory published today.

"The vulnerability could have allowed an attacker to perform remote command execution across IR infrastructure not limited to a single tenant," the company added in a Microsoft Security Response Center (MSRC) blog post.

Successful exploitation of this ODBC connector for Amazon Redshift flaw could let malicious attackers running jobs in a Synapse pipeline execute remote commands.

In the next attack stage, they could potentially steal the Azure Data Factory service certificate to execute commands in another tenant's Azure Data Factory Integration Runtimes.

"Based on our understanding of the architecture of the service, and our repeated bypasses of fixes, we think that the architecture contains underlying weaknesses that should be addressed with a more robust tenant separation mechanism," Orca Security's Avi Shua said (https://orca.security/resources/blog/azure-synapse-analytics-security-advisory/).

"Until a better solution is implemented, we advise that all customers assess their usage of the service and refrain from storing sensitive data or keys in it."

How to mitigate

Microsoft says that customers using Azure cloud (Azure Integration Runtime) or who host their own on-premises (Self-Hosted Integration Runtime) with auto-updates turned on don't need to take any further action to mitigate this flaw.

Self-host IR customers who don't have auto-update toggled on were already notified to safeguard their deployments via Azure Service Health Alerts (ID: MLC3-LD0).

The company advises them to update their self-hosted IRs to the latest version (5.17.8154.2) available on Microsoft's Download Center (https://www.microsoft.com/en-us/download/details.aspx?id=39717).

These updates can be installed on 64-bit systems with .NET Framework 4.7.2 or above running client and server platforms, including the latest releases (Windows 11 and Windows Server 2022).

"For additional protection, Microsoft recommends configuring Synapse workspaces with a Managed Virtual Network which provides better compute and network isolation," Redmond added (https://msrc-blog.microsoft.com/2022/05/09/vulnerability-mitigated-in-the-third-party-data-connector-used-in-azure-synapse-pipelines-and-azure-data-factory-cve-2022-29972/).

"Customers using Azure Data Factory can enable Azure integration runtimes with a Managed Virtual Network."

You can find further information on how to fully mitigate CVE-2022-299 in the "Customer Recommendations and Additional Support (https://msrc-blog.microsoft.com/2022/05/09/vulnerability-mitigated-in-the-third-party-data-connector-used-in-azure-synapse-pipelines-and-azure-data-factory-cve-2022-29972/#:~:text=command%20line%20activity.-,Customer%20Recommendations%20and%20Additional%20Support,-To%20ensure%20that)" section of MSRC's blog post.

"Unfortunately, our research leads us to believe that the underlying architectural weakness is still present. There are areas in the service where a huge amount of Microsoft and 3rd party code, runs with SYSTEM permissions, processing customer controlled input," Shua added.

"This runs on shared machines with access to Azure service keys and sensitive data of other customers. These areas of the service only have application-level separation and lack sandbox or hypervisor-level isolation. This is a major attack surface and not consistent with the level of security that public cloud customers expect."

Disclosure timeline:

- January 4 – Orca reported the issue to Microsoft
- March 2 – Microsoft completed rollout of initial hotfix
- March 11 – Microsoft identified and notified the customer affected by the researcher's activity

- March 30 – Orca notified Microsoft of an additional attack path to the same vulnerability
- April 13 – Orca notified Microsoft of a second attack path to the same vulnerability
- April 15 – Additional fixes deployed for the two newly reported attack paths as well as additional defense in depth measures applied

In March, Microsoft said it fixed another Azure security vulnerability in December (also reported by Orca Security) that enabled attackers to take complete control over other Azure customers' data by abusing an Azure Automation service bug dubbed AutoWarp (https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-critical-azure-bug-that-exposed-customer-data/).

Last month, the company addressed a chain of critical bugs reported by cloud security firm Wiz in the Azure Database for PostgreSQL Flexible Server (known as ExtraReplica (https://www.bleepingcomputer.com/news/security/microsoft-fixes-extrareplica-azure-bugs-that-exposed-user-databases/)) that let malicious users gain access to other customers' databases after bypassing authentication.

Other Microsoft Azure flaws fixed by Redmond during the last year also include ones Wiz researchers found in Azure Cosmos DB (https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-azure-customers-of-critical-cosmos-db-vulnerability/), the Open Management Infrastructure (OMI) software agent (https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-critical-bugs-in-secretly-installed-azure-linux-app/), and the Azure App Service (https://www.bleepingcomputer.com/news/security/microsoft-azure-app-service-flaw-exposed-customer-source-code/).

Update: Clarified ExtraReplica attribution.