Security Advisory 2022-033

Critical RCE Vulnerabilities in Microsoft Azure Synapse

May 10, 2022 — v1.0

TLP:WHITE

History:

- *10/05/2022 — v1.0 – Initial publication*

Summary

On May 9th, Microsoft issued one security advisory addressing a critical RCE vulnerability in the third-party Open Database Connectivity (ODBC) driver used to connect to Amazon Redshift in Azure Synapse pipelines and Azure Data Factory Integration Runtime (IR) [1]. This vulnerability CVE-2022-29972 has CVSS score of 8.2 out of 10 and it may allow an attacker to perform remote command execution across IR infrastructure not limited to a single tenant.

According to Microsoft article [2], there was no evidence of misuse or malicious activity. Only self-host IR environments without auto-update need to take action to safeguard their deployments.

Technical Details

The vulnerability in the third-party ODBC connector for Amazon Redshift allowed a user running jobs in a Synapse pipeline to execute remote commands. A user who exploited this vulnerability could then potentially acquire the Azure Data Factory service certificate and execute commands in another tenant's Azure Data Factory Integration Runtimes. These certificates are specific to Azure Data Factory and Synapse Pipelines, and do not pertain to the rest of Azure Synapse.

Exploiting this vulnerability requires an attacker to have at least one of the following roles:

- Synapse Administrator
- Synapse Contributor
- Synapse Compute Operator

Affected Products

Azure Data Factory with Self-hosted IRs (SHIRs) with a version less than 5.17.8154.2.

SHIRs with auto-update enabled or using Azure IRs are already mitigated.

Recommendations

Azure Data Factory with Self-hosted IRs (SHIRs) with auto-update turned off must update their SHIRs to the latest version (5.17.8154.2) that can be found here [3]. 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

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29972

[2] 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/

[3] https://www.microsoft.com/en-us/download/details.aspx?id=39717