Security Advisory 2021-045

Microsoft - Cosmos DB Vulnerability

August 31, 2021 — v1.0

TLP:WHITE

History:

- *31/08/2021 — v1.0 – Initial publication*

Summary

On the 26th of August 2021, a cloud security company Wiz announced a vulnerability in Microsoft Azure managed database service - Cosmos DB [1]. When exploited, it gives read/write access to Cosmos DB credentials, including primary key, which provide complete and unrestricted remote access to Microsoft Azure databases and accounts.

Technical Details

The vulnerability dubbed ChaosDB is caused by a chain of bugs in the Jupyter Notebook feature, enabled by default and designed to help customers visualise data. Details are provided on researchers' dedicated page [1].

Products Affected

Cosmos DB account that uses the Jupyter Notebook feature feature.

Recommendations

Microsoft has already warned cloud customers that hackers may have potentially accessed their data via an exploitable vulnerability in its Azure cloud service.

To mitigate the risk and block potential attacks, Microsoft advises Azure customers to regenerate the Cosmos DB Primary Keys that could have been stolen before the vulnerable feature was disabled [2].

The company also advised customers to take the following recommended actions to further secure their Azure Cosmos DB databases [3]:

- Schedule a regular rotation and regeneration of your primary and secondary keys.
- Consider using the Azure Cosmos DB firewall and virtual network integration to control the access to your accounts at the network level.
- If you are using the Azure Cosmos DB Core (SQL) API, consider using the Azure Cosmos DB role-based access control (RBAC) to authenticate your database operations with Azure

Active Directory instead of primary/secondary keys. With RBAC, you have the option to completely disable your account's primary/secondary keys.

Reviewing all past activity on the Cosmos DB accounts is also recommended to detect previous attempts to exploit this vulnerability.

Considering the seriousness of the flaw, and the fact that **exploits are already available**, CERT-EU strongly advises to **apply recommendations as soon as possible**.

References

[1] https://www.wiz.io/blog/chaosdb-how-we-hacked-thousands-of-azure-customers-databases

[2] https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to-data?tabs=using-primary-key#primary-keys

[3] https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-azure-customers-of-critical-cosmos-db-vulnerability/