UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00189

COSMOS DB CRITICAL MICROSOFT AZURE BUG

DATE ISSUED: 30th August 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Researchers at Wiz have discovered an exploitable vulnerability in Microsoft Azure's Cosmos DB that has been present for some months, dubbed #ChaosDB, which could allow full remote account takeover with admin rights. The component has since been disabled by Microsoft, who are advising anyone who runs Cosmos DB to assume they have been exposed and to investigate immediately.

BREAKDOWN

According to the researchers, any Azure customer would have been able to access another's without authentication. The issues stems from Jupyter Notebooks which is directly integrated with the Azure portal for added convenience, and while running queries it was possible to gain credentials for the Jupyter Notebook Storage account for other users, their databases and primary read/write keys used for encryption. #ChaosDB is made up of a daisy-chain style attack and details regarding this have not been provided to the general public. While there is no evidence of exploitation in the wild as yet, Wiz were awarded $40K for the discovery.

REMEDIATION STEPS

- Regenerate CosmosDB primary keys using instructions found in Microsoft sources below
- Review past activity history in your account to investigate whether you have been breached.

REFERENCES & RESOURCES

Microsoft https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to-data?tabs=using-primary-key#primary-keys
https://gotcosmos.com/about/customers
Threatpost https://threatpost.com/azure-cosmos-db-bug-cloud/168986/