

Detecting a vulnerability that makes 3,000 companies using Microsoft Azure vulnerable to hackers reading data over the past 2 years

Using Microsoft Azure can help companies better secure their data. However, a newly discovered vulnerability shows the opposite result.

Microsoft has just been forced to notify more than 3,000 organizations and businesses, including giants like ExxonMobil, Walgreens, Coca Cola, Symantec, Zeiss. about potential security risks.

Specifically, the Azure platform that the above businesses are using has a vulnerability that allows any hacker access to read, edit, and delete data stored on Azure Cosmos DB database for more than 2 years. past 2 years.



This vulnerability was discovered by security company Wiz and named "ChaosDB". It is related to a series of configuration errors in the display feature of Jupiter Notebook, which Microsoft added to Cosmos DB in 2019. Jupiter Notebook is enabled by default in all installations of Cosmos DB.

Wiz reported the issue to Microsoft on August 12. By August 14, Microsoft had found a fix. Up to now, according to Microsoft, there is no sign of this vulnerability being exploited by hackers.

After discovering the problem, Wiz advised all companies using Cosmos DB to regenerate the access key and take other security measures. Businesses should double-check Cosmos DB security measures even if your business doesn't receive a warning from Microsoft.

Microsoft also rewarded Wiz \$40,000 for reporting the vulnerability to them.

You finished reading the article "**Detecting a vulnerability that makes 3,000 companies using Microsoft Azure vulnerable to hackers reading data over the past 2 years**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
