8-Reuters-Researchers, cybersecurity agency

By Joseph Menn

3 minute read

Smartphone is seen in front of Microsoft logo displayed in this illustration taken, July 26, 2021. REUTERS/Dado Ruvic/Illustration

Aug 28 (Reuters) - Researchers who discovered a massive flaw in the main databases stored in Microsoft Corp's (MSFT.O) Azure cloud platform on Saturday urged all users to change their digital access keys, not just the 3,300 it notified this week.

As first reported by Reuters , researchers at a cloud security company called Wiz discovered this month they could have gained access to the primary digital keys for most users of the Cosmos DB database system, allowing them to steal, change or delete millions of records. read more

Alerted by Wiz, Microsoft rapidly fixed the configuration mistake that would have made it easy for any Cosmos user to get into other customers' databases, then notified some users Thursday to change their keys *[Rebuild]*.

In a blog post Friday, Microsoft said it warned customers *[Rebuild]* which had set up Cosmos access during the weeklong research period. It found no evidence that any attackers had used the same flaw to get into customer data, it noted.

“Our investigation shows no unauthorized access other than the researcher activity,” Microsoft wrote. “Notifications have been sent to all customers that could be potentially affected due to researcher activity *[Rebuild]*,” it said, perhaps referring to the chance that the technique had leaked from Wiz.

“Though no customer data was accessed, it is recommended you regenerate your primary read-write keys *[Rebuild]*,” it said.

The U.S. Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency used stronger language in a bulletin Friday, making clear it was speaking not just to those notified.

“CISA strongly encourages Azure Cosmos DB customers to roll and regenerate their certificate key,” the agency said .

Experts at Wiz, founded by four veterans of Azure’s in-house security team, agreed.

“In my estimation, it’s really hard for them, if not impossible, to completely rule out that someone used this before *[Worry]*,” said one of the four, Wiz Chief Technology Officer Ami Luttwak. At Microsoft he developed tools for logging cloud security incidents.

Microsoft did not give a direct answer when asked if it had comprehensive logs for the two years when the Jupyter Notebook feature was misconfigured, or had used another way to rule out access abuse.

“We expanded our search beyond the researcher’s activities to look for all possible activity for current and similar events in the past *[Rebuild]*,” said spokesman Ross Richendrfer, declining to address other questions *[Deny]*.

Wiz said Microsoft had worked closely with it on the research but had declined to say how it could be sure earlier customers were safe.

[Worry]

“It’s terrifying. I really hope than no one besides us found this bug, *[Worry]*” said one of the lead researchers on the project at Wiz, Sagi Tzadik.