BUSINESS INSURANCE.

Microsoft warns thousands of cloud customers of exposed databases

Posted On: Aug. 27, 2021 10:40 AM CST

(Reuters) — Microsoft on Thursday warned thousands of its cloud computing customers, including some of the world's largest companies, that intruders could have the ability to read, change or even delete their main databases, according to a copy of the email and a cybersecurity researcher.

The vulnerability is in Microsoft Azure's flagship Cosmos DB database. A research team at security company Wiz discovered it was able to access keys that control access to databases held by thousands of companies. Wiz Chief Technology Officer Ami Luttwak is a former chief technology officer at Microsoft's Cloud Security Group.

Because Microsoft cannot change those keys by itself, it emailed the customers Thursday telling them to create new ones. Microsoft agreed to pay Wiz $40,000 for finding the flaw and reporting it, according to an email it sent to Wiz.

"We fixed this issue immediately to keep our customers safe and protected. We thank the security researchers for working under coordinated vulnerability disclosure," Microsoft told Reuters.

Microsoft's email to customers said there was no evidence the flaw had been exploited. "We have no indication that external entities outside the researcher (Wiz) had access to the primary read-write key," the email said.

“This is the worst cloud vulnerability you can imagine. It is a long-lasting secret,” Mr. Luttwak told Reuters. “This is the central database of Azure, and we were able to get access to any customer database that we wanted.”

Mr. Luttwak's team found the problem, dubbed ChaosDB, on Aug. 9 and notified Microsoft Aug. 12, Mr. Luttwak said.

The flaw was in a visualization tool called Jupyter Notebook, which has been available for years but was enabled by default in Cosmos beginning in February. After Reuters reported on the flaw, Wiz detailed the issue in a blog post.

Mr. Luttwak said even customers who have not been notified by Microsoft could have had their keys swiped by attackers, giving them access until those keys are changed. Microsoft only told customers whose keys were visible this month, when Wiz was working on the issue.

Microsoft told Reuters that "customers who may have been impacted received a notification from us," without elaborating.

The disclosure comes after months of bad security news for Microsoft. The company was breached by the same suspected Russian government hackers that infiltrated SolarWinds, who stole Microsoft source code. Then a wide number of hackers broke into Exchange email servers while a patch was being developed.

A recent fix for a printer flaw that allowed computer takeovers had to be redone repeatedly. Another Exchange flaw last week prompted an urgent U.S. government warning that customers need to install patches issued months ago because ransomware gangs are now exploiting it.

Problems with Azure are especially troubling, because Microsoft and outside security experts have been pushing companies to abandon most of their own infrastructure and rely on the cloud for more security.

But though cloud attacks are more rare, they can be more devastating when they occur. What's more, some are never publicized.

A federally contracted research lab tracks all known security flaws in software and rates them by severity. But there is no equivalent system for holes in cloud architecture, so many critical vulnerabilities remain undisclosed to users, Mr. Luttwak said.