Remember the Y2K bug? Microsoft confirms new Y2K22 issue

Microsoft says it is aware of a programming flaw which saw some customers’ Exchange servers stop processing emails just as the clock struck midnight on New Year’s Eve.

System administrators, who are sharing workarounds on social media, have dubbed the bug Y2K22 – in the style of the Y2K bug which affected some computers at exactly the same time 22 years earlier.

Microsoft said its engineers had been “working around the clock on a fix” that wouldn’t require customers to fiddle with their on-premise servers to get things moving again, but warned they found this “would require several days to develop and deploy”.

Instead, those engineers are now working on a different update “which is in final test validation” that will require customer action, but also offer “the quickest time to resolution”.

Y2K: What damage did the 'Millennium Bug' really cause?

PODCAST

What actually went wrong?

The technical issue seems to lie with the way that Microsoft was naming updates for its malware-scanning engine, putting the year, month, and day (220101) at the front of another four-digit number (0001).

Microsoft seems to use this system because when an update is named "2,201,010,001" it is simple to mathematically check which update is the most recent as it will have the higher value.

The problem appears to be that the field this number was stored in had a limit of being 31 bits, meaning the highest number that could be represented was 2,147,483,648 or 2 to the power of 31.

As soon as the clock ticked over to 2022, this naming system was going to exceed the maximum value that could be represented in 31 binary symbols.

The company hasn’t yet confirmed the technical details, but its explanation seems to support the theory: “The version checking performed against the signature file is causing the malware engine to crash, resulting in messages being stuck in transport queues.”

Image:
The only workaround currently is turning off Microsoft’s anti-malware features
What problems has it caused?

The software update affected is related to Microsoft’s anti-malware scanning software, meaning that messages which should be queued up and checked are simply being queued.

One managed service provider warned on Microsoft’s site that their company had seen a client queue 10,000 messages in less than 24 hours.

They said this risked filling up the server’s storage and making it crash, potentially taking the business offline.

“Don’t wait for the Microsoft patch if you are not sure your Exchange Server storage has the capacity to hold all queued messages without filling up disks and crashing,” they wrote.

“Apply the workaround now to release the messages sooner than later.”

The problem is the workaround involves disabling the malware filtering feature – potentially exposing companies to hackers.

Microsoft warns: “You should use one of these workarounds only if you have an existing malware scanner for email other than the engine in Exchange Server.”

The Microsoft Exchange team said: “We expect to have this update to you shortly along with the actions required by you. We are sorry for any inconvenience that this issue has caused.”