Vulnerability causes Exchange servers to 'crash' around the world: Microsoft offers a fix method

This issue was first reported by a Reddit member at 1 a.m. EST.

Update on 03/01: Microsoft has released the patch

So just over a day after major technology news sites simultaneously reported that Exchange server systems around the world had problems within the first hours of the new year 2021, Microsoft has released a patch. fix problem.

This is basically a date value handling error, when the newly selected value of "2.201.010.001" exceeds what the Server can handle with the current Int32 data type. This resulted in the malware checking engine crashing, and as a result, emails and messages getting stuck in the transport queue on Exchange 2016 and 2019 server systems, with event log errors. 5300 and 1106 (FIPFS).

The solution offered by Microsoft is to use the automatic scan engine reset script, or manual input.

Method 1: Use the automatic scan engine reset script (available at here). This command can be run in parallel on multiple servers. A successful script completion will produce the following output:

```
[PS] C:/Program Files/Microsoft/Exchange Server/V15/Scripts>./Reset-ScanEngineVe
```

Method 2: Manually fix errors

Remove existing tools and metadata

1. Stop the Microsoft Filtering Management service. When prompted to stop the Microsoft Exchange Transport service, click Yes.
2. Use Task Manager to shut down and make sure that the Updervice.exe process is not running.
3. Delete the following folder: %ProgramFiles%/Microsoft/Exchange Server/V15/FIP-FS/Data/Engines/amd64/Microsoft.
4. Delete all files from the following directory: %ProgramFiles%/Microsoft/Exchange Server/V15/FIP-FS/Data/Engines/metadata.

Update to the latest engine

1. Start the Microsoft Filtering Management and Microsoft Exchange Transport services.
2. Open the Exchange Management Shell, navigate to the Scripts folder (%ProgramFiles%/Microsoft/Exchange Server/V15/Scripts), and run Update-MalwareFilteringServer.ps1 .

Verify engine update information

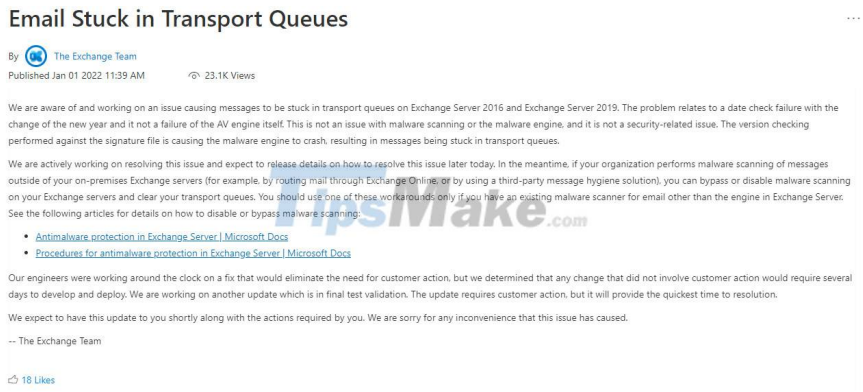
1. In the Exchange Management Shell, run Add-PSSnapin Microsoft.Forefront.Filtering.Management.Powershell.
2. Run Get-EngineUpdateInformation and verify the UpdateVersion information is 2112330001.

You can find more details on the official Microsoft blog HERE.

January 1, 2021:

For most people, the new year is a time to gather with family and friends, or simply relax and think about future plans. However, for the sysadmins responsible for Exchange servers around the world, this new year can be a 'sad anniversary' as Microsoft's server service has just experienced a serious system problem, leading to a major system crash. to global disruption.

This issue was first reported by a Reddit user with the nickname /u/FST-LANE at 1 a.m. EST. It mentioned that Microsoft had released an invalid update for the Exchange system, with the identifier '220101001'. This was presumably a scheduled patch to allow the system to process the new day's data, but it didn't go as planned. 'I observed a bunch of errors from the FIPFS service saying: Cannot convert '220101001' to long', said the /u/FST-LANE member.



Email Stuck in Transport Queues

By The Exchange Team

Published Jan 01 2022 11:39 AM 23.1K Views

We are aware of and working on an issue causing messages to be stuck in transport queues on Exchange Server 2016 and Exchange Server 2019. The problem relates to a date check failure with the change of the new year and it not a failure of the AV engine itself. This is not an issue with malware scanning or the malware engine, and it is not a security-related issue. The version checking performed against the signature file is causing the malware engine to crash, resulting in messages being stuck in transport queues.

We are actively working on resolving this issue and expect to release details on how to resolve this issue later today. In the meantime, if your organization performs malware scanning of messages outside of your on-premises Exchange servers (for example, by routing mail through Exchange Online, or by using a third-party message hygiene solution), you can bypass or disable malware scanning on your Exchange servers and clear your transport queues. You should use one of these workarounds only if you have an existing malware scanner for email other than the engine in Exchange Server. See the following articles for details on how to disable or bypass malware scanning:

- Antimalware protection in Exchange Server | Microsoft Docs
- Procedures for antimalware protection in Exchange Server | Microsoft Docs

Our engineers were working around the clock on a fix that would eliminate the need for customer action, but we determined that any change that did not involve customer action would require several days to develop and deploy. We are working on another update which is in final test validation. The update requires customer action, but it will provide the quickest time to resolution.

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.

-- The Exchange Team

18 Likes

This is also consistent with more in-depth reports from Marius Sandbu, system manager from Norway who was one of the first experts to observe the problem, as well as giving a basic summary report on the problem. problem cause. Sandbu discovered that the Microsoft Exchange servers had suddenly stopped processing mail altogether starting at 00:00 on January 1, 2022. The reason for this fatal problem is most likely because Microsoft is using int32 for the date and with the new value of 2,201,010.001, exceeds the maximum value of int "long" of 2,147,483,647".

The problem here is the stopping distance solution. In order for the Exchange server to continue processing mail, sysadmins are forcibly disabling malware scanning on their systems:

> 'Currently, it seems that the main solution is to disable the anti-malware scanner on the Exchange Server using Set-MalwareFilteringServer -BypassFiltering $True -identity and restart the Microsoft Exchange Transport service'.

However, this can leave users, and possibly the servers themselves, vulnerable to flash malicious attacks.

This bug affects Exchange Server 2013. 2016 and 2019. Microsoft has now confirmed the issue and is working on a fix.