Introducing Exchange Server 2019, how to install Exchange Server 2019

Exchange Server 2019 is designed to deliver security, performance, and improved manageability and operations - properties Microsoft's biggest customers have come to expect from Exchange.

Microsoft released a new version of Exchange Server in 2019. It brings a number of new features to the mail and calendar server, including security and performance improvements. To help you decide whether the new version is right for you, **Tipsmake** will summarize what you need to know about Exchange Server 2019 through the following article!

What is Exchange Server 2019?

Exchange Server 2019 is designed to deliver security, performance, and improved manageability and operations - properties that Microsoft's biggest customers have come to expect from Exchange.

Main features of Exchange Server 2019

Windows Server Core

Support for Windows Server Core is finally coming to this release! Exchange Server 2019 can now be installed on Windows Server 2016 and 2019 Core, providing a secure platform for Exchange. The Exchange team recommends this as the best option for installing Exchange Server 2019. The GUI interface will still be available. It's important to note that Exchange 2019 can only be installed on Windows Server 2019.

Efficiency

Exchange 2019 will support up to 48 CPU cores and 256GB of memory to take advantage of the new hardware developments. This is a huge increase over Exchange 2016, which only supports 24 CPU cores and 192GB of memory. Larger organizations will be able to deploy fewer Exchange servers to save licensing costs and reduce data center size.

Microsoft has incorporated Bing search technology to improve the search experience. The index is now part of the mailbox database, eliminating the need to manage additional log files and the need to rebuild the content index. This will help reduce database failover time caused by mailbox database replication.

End user experience

Exchange 2019 will have a number of enhancements included in Exchange Online, such as **Do Not Forward** and **Simplified Calendar Sharing** . Additionally, Microsoft is adding the ability for administrators to manage user's calendar events and to assign and authorize permissions more easily through the new PowerShell cmdlets.

Unified Messaging

Microsoft has removed the Unified Messaging role from Exchange 2019. Exchange 2019 will not support the use of third-party PBX or Skype for Business Server for Exchange Server. This means if you require voicemail functionality, you have two options: Migrate to Skype for Business Server 2019 using Cloud Voicemail or migrate to Office 365 with Cloud Voicemail. And the good news: Microsoft has implemented a number of ways to reduce costs when it comes to switching to Cloud Voicemail.

How to install Exchange Server 2019

All Exchange Server admirers and those interested are aware of the latest version of Exchange Server i.e. Exchange 2019. Its advanced features and security measures are attracting Exchange users looking for it. change. Below I will guide you through the manual process for installing Exchange Server 2019.

Manual installation of Exchange Server 2019

Several requirements need to be met by an Exchange user or administrator before starting the Exchange Server 2019 installation process. The main prerequisites include:

Hardware requirements

1. 64-bit Intel processor (EM64T), 64-bit AMD processor
2. 30GB minimum free disk space
3. 128GB minimum storage (for Mailbox), 64GB (for Edge Transport)
4. NTFS file system
5. Screen resolution of 1024 x 768

Software requirement

Required operating system

1. Mailbox and Exchange Transport: Windows Server 2019 Standard / Data Center
2. Management tool: Windows 10 (64-bit) or Windows Server 2019 Standard / Data Center

Requires Outlook Client

1. Outlook 2013 / Outlook 2016 / Outlook 2016 for Mac / Outlook 2019 / Outlook (Mac) for Office 365

Requirements for network & directory servers

1. Active Directory Forests: Windows Server 2012 R2 or later versions
2. Active Directory Site with a Writable Domain Controller that cannot be deleted
3. Domain Controller: Windows Server 2019 Standard / Windows Server 2016
4. Standard / Windows Server 2012 R2 Standard
5. DNS Namespace: Contiguous / Non-Contiguous / Disjoint / Single label domain
6. IPv6 Support: Requires both IPv4 and IPv6

When all of the above requirements have been met, the Exchange administrator can continue to prepare the Active Directory.

For small organizations, it is enough to move to the Exchange setup phase as a member of the Schema Admin as well as the Enterprise Admin security groups.

But for larger organizations with multiple mailboxes, an Active Directory environment needs to be prepared before going through the Exchange setup process.

Prepare the Active Directory environment for Exchange 2019

Step 1. First, install the .NET framework (4.7.2 or 4.7.1), Visual C ++ Redistributable Packages for Visual Studio and the Unified Communications Managed API on your Exchange system.

Step 2. After all above software requirements are installed, reboot the system.

Step 3. Launch Windows PowerShell (as admin). Here, run the command as shown below.

```
Install-WindowsFeature RSAT-ADDS
```

Step 4. The next step is to run another command in Windows PowerShell to install the Server requirements.

```
Install-WindowsFeature NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clus
```

Step 5. Now, mount Exchange Server 2019 Preview Installation Media on the system.

Step 6. Type **cmd** in the **Search** box , right-click on **Command Prompt** and select the option **Run as administrator** . On the **Command Prompt** window that opens, run the following command:

```
Setup.exe /PrepareSchema /IAcceptExchangeServerLicenseTerms
```

Step 7. Next, run this last command to prepare the domain:

```
Setup.exe /PrepareAllDomains /IAcceptExchangeServerLicenseTerms
```

Step 8. You have successfully prepared an Active Directory environment (Schema and Domain) to install Exchange Server 2019.

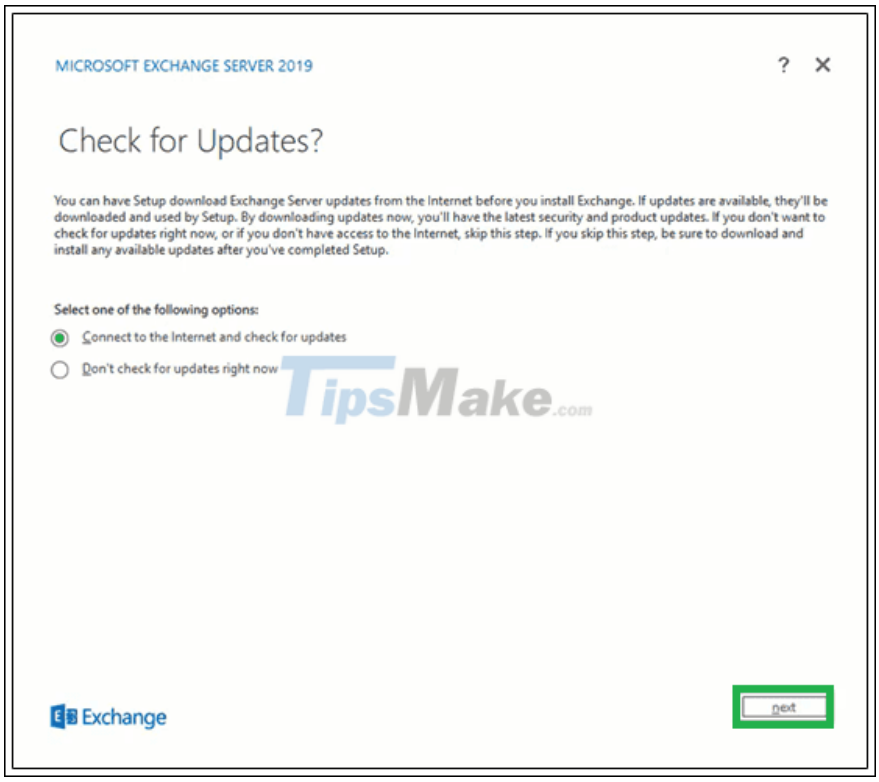
Now you need to move on to setting up Exchange Server with the application setup on the Exchange system.

Exchange Server 2019 installation and setup process

Follow these steps to complete the Exchange 2019 setup.

Step 1. Go to **Setup.exe** , double-click it to start the installation process.

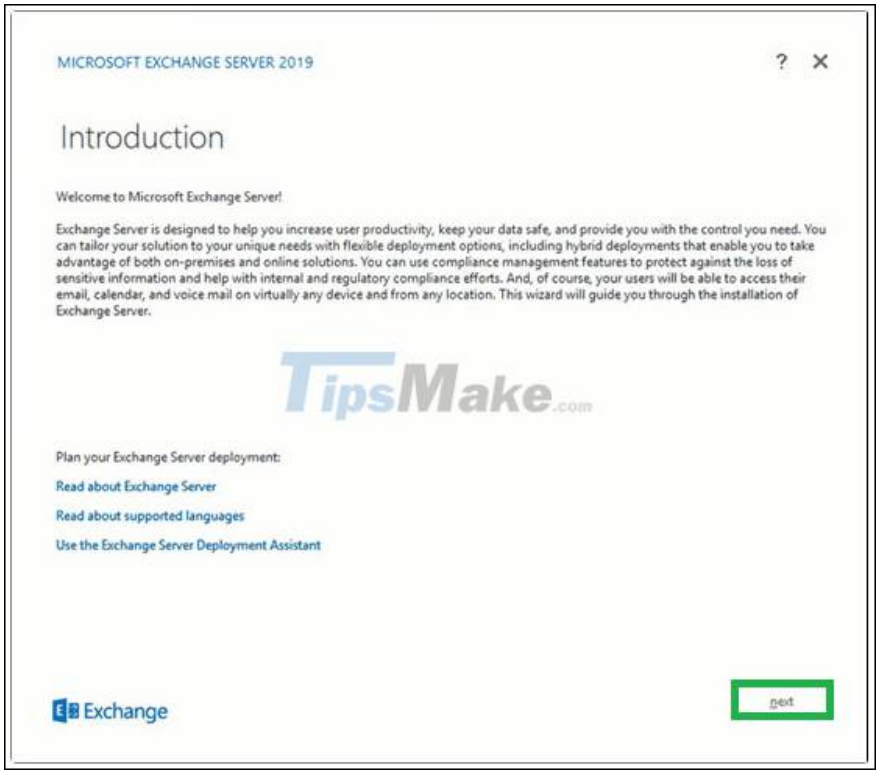
Step 2. Go to the window **Check for updates?** Next, choose one of the options - **Connect to the Internet and check for updates** and **Don't check for updates right now** as needed and click **Next.**



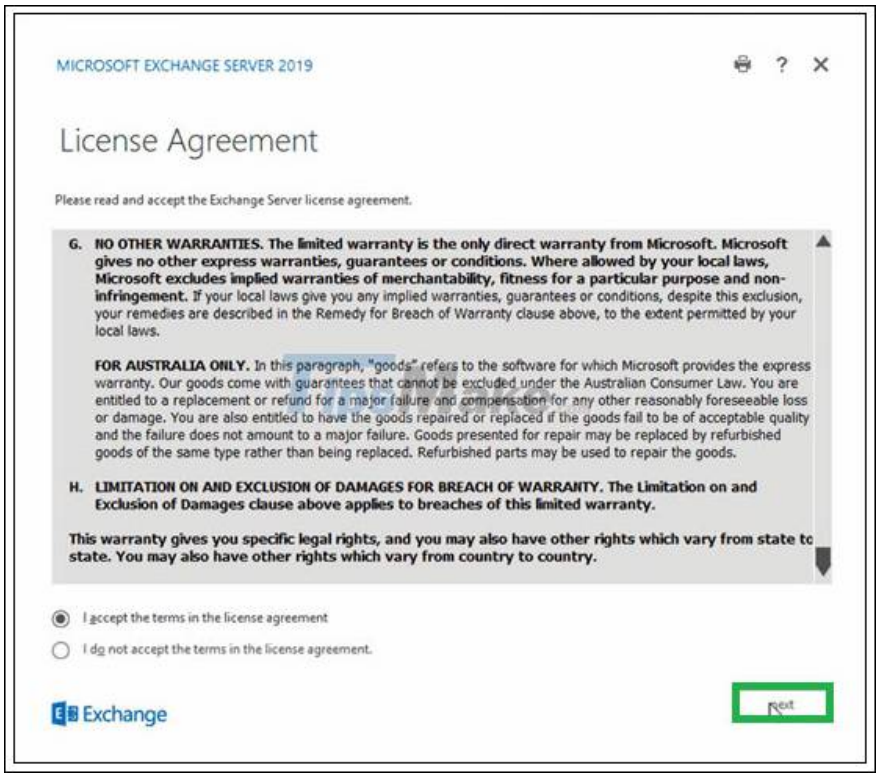
Step 3. Next, the process of copying the Exchange files required to install Exchange Server will begin. Let's see the process!

Step 4. The **Initializing Setup** screen will be displayed next.

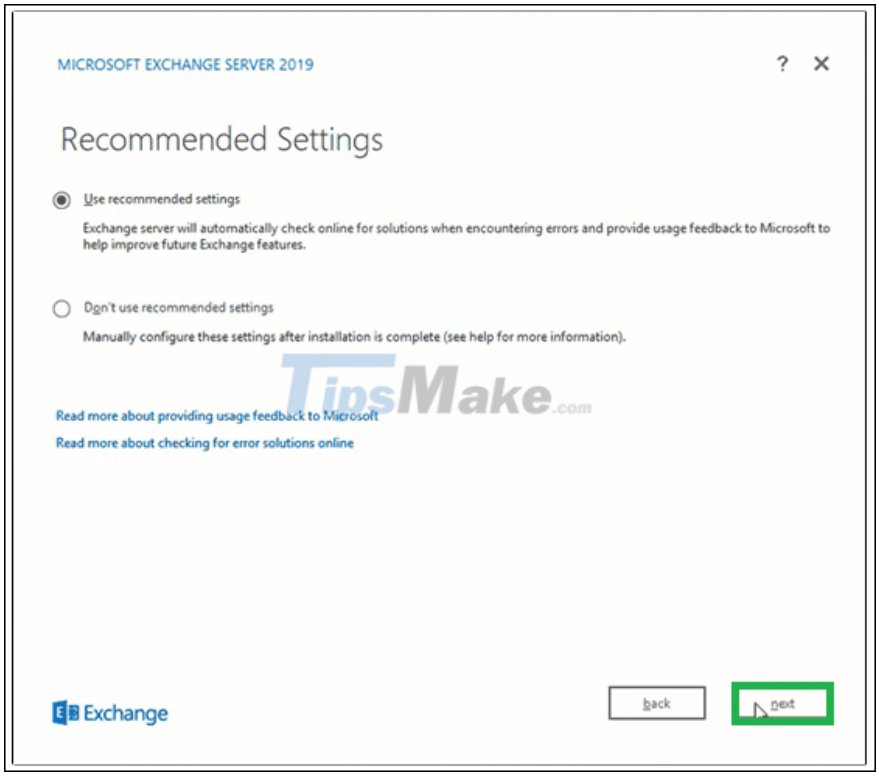
Step 5. You should now see the introduction page for Exchange Server 2019. Read this brief introduction. You can click on the links provided for more information. Click **Next** to continue.



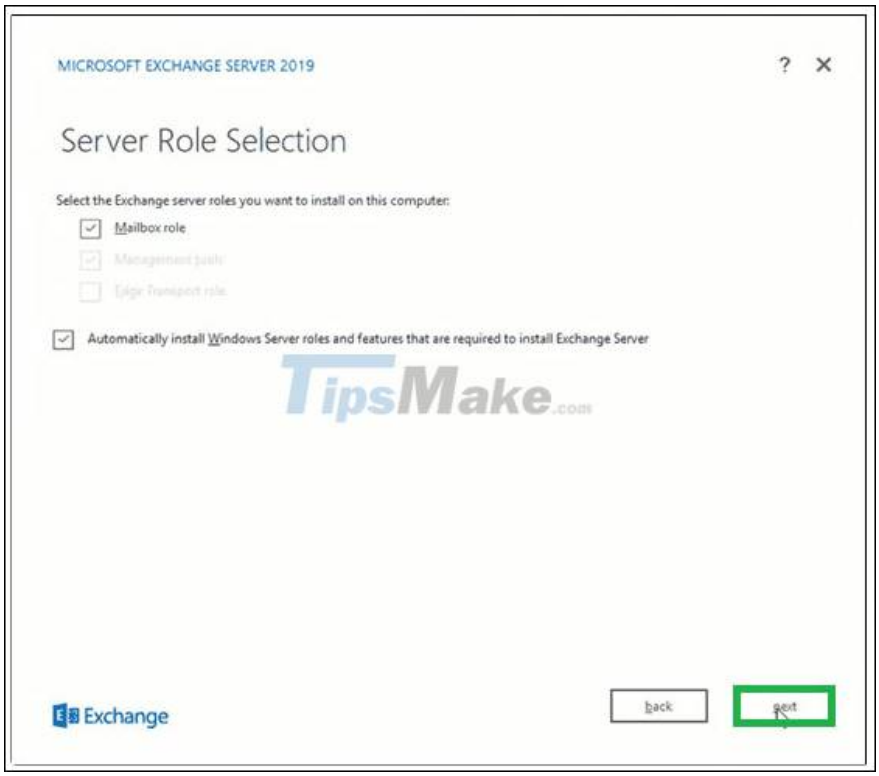
Step 6. On the **License Agreement** page , read all the instructions, select the option to accept the terms in the license agreement and click **Next.**



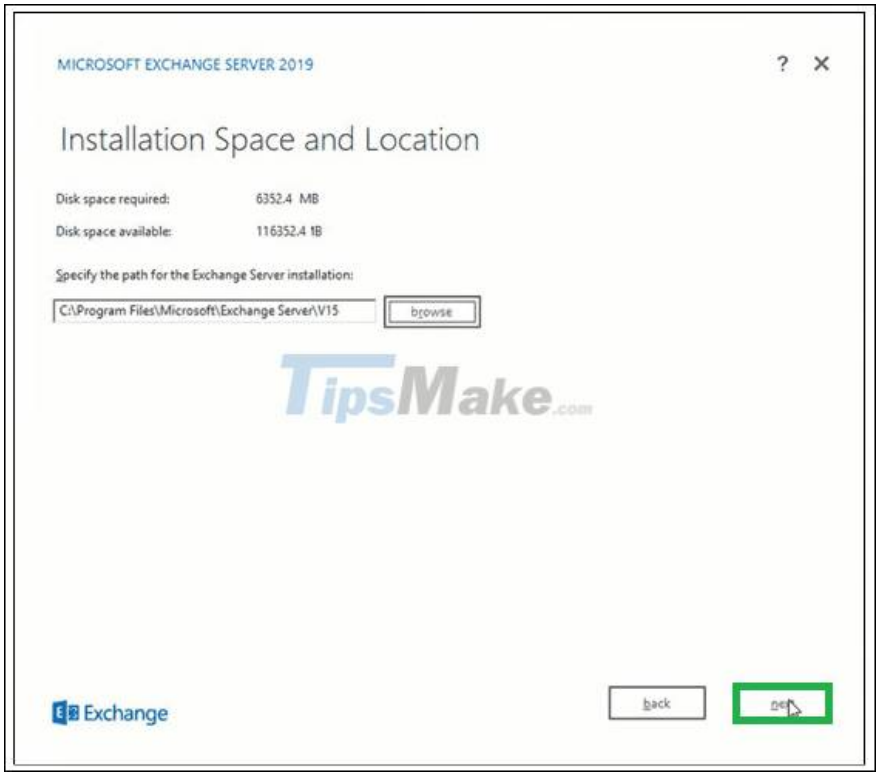
Step 7. On the **Recommendation Settings** page , select the **Use recommendation settings option** and click **Next.**



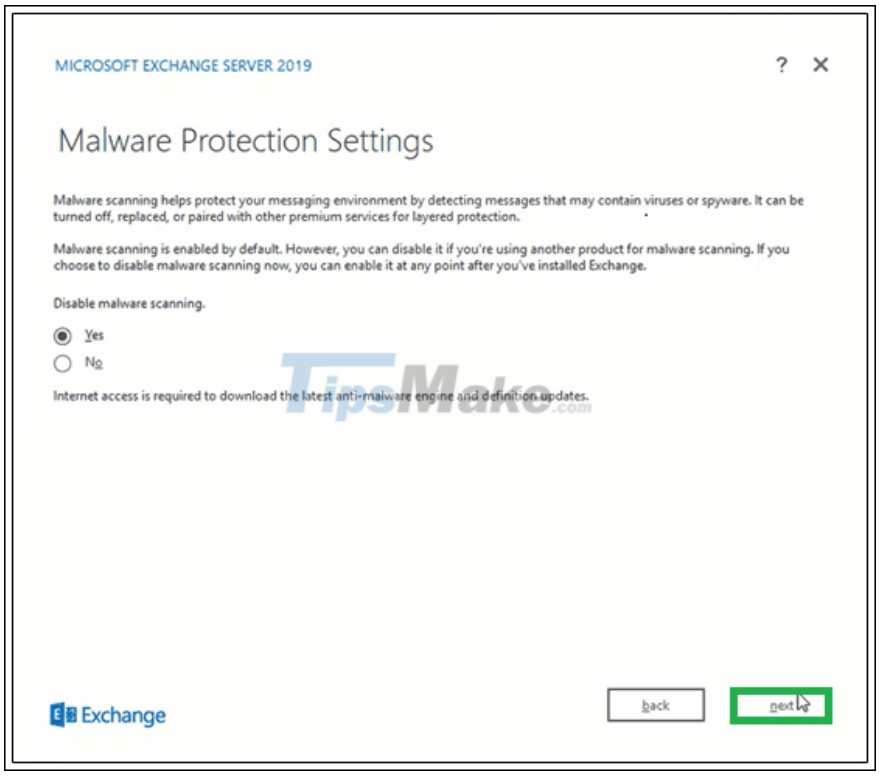
Step 8. Here, select the **Mailbox role** option in the **Exchange Server roles section** and select the **Automatically install Windows Server roles and features** check box **that are required to install Exchange Server** . Click **Next.**



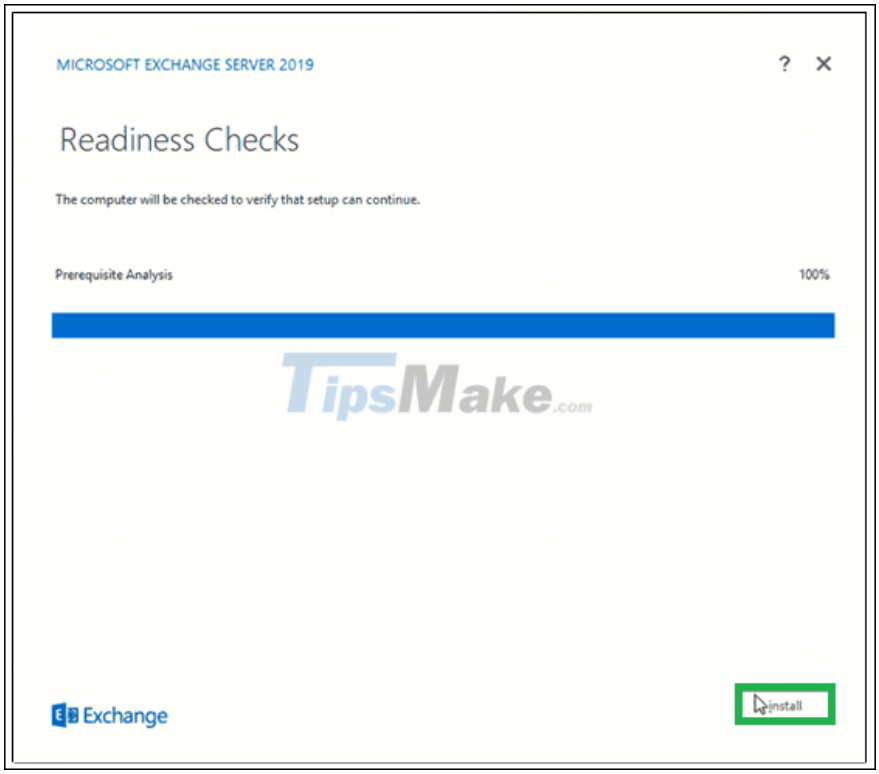
Step 9. Click Browse to specify the path for the Exchange Server installation or leave it at the default selected path. Click **Next.**



Step 10. For **Malware Protection Settings** , select the **Yes** or **No option** (to disable malware scanning) and click **Next.**



Step 11. Wait for the **Readiness Checks** process to complete to verify the settings and then click **Install.**



Step 12. The **Progress Setup** will begin copying the Exchange files.

Step 13. Once the setup is complete, it will display the **Setup Completed** page **.**

To start Exchange Server immediately, select the **Launch Exchange Administration Center after Finishing Exchange setup** check box . Click **Finish.**

Exchange Server 2019 has been successfully installed on your system. By running these two commands in the Exchange Management Shell, you will get complete information about your newly installed Exchange Server.

```
Get-ExchangeServer Get-ExchangeServer -Identity MailboxName | Format-List
```

An Exchange 2019 administrator can also log in to the Exchange Admin Center to confirm a successful Exchange Server installation.

Note : Exchange administrators are required to follow the following installation tasks for Exchange Server, such as providing Exchange product key, installing Exchange management tools on client computer, registering Edge, configuring security certificate , etc.

Things to know about Microsoft Exchange Server hack

On March 2, 2021, Microsoft released an emergency patch to fix 4 extremely critical zero-day vulnerabilities in Exchange Server version 2013/2016/2019. All four of these vulnerabilities were previously being actively exploited by a hacker group called HAFNIUM. Along with that is the participation of a series of other unknown hacker groups, creating a large-scale attack campaign that can have extremely serious consequences for Microsoft and partners around the world.

There is absolutely no evidence to link this Exchange Server campaign to the SolarWinds supply chain attack that affected more than 18,000 organizations worldwide shortly before. However, a delay in patching vulnerable Exchange Server servers can have the same, or worse, impact on global businesses.

Here's everything you need to know about security issues as well as expert guidance on this serious case.

What happened to Exchange Server?

Early January 2021: Microsoft uncovered the first clues about four zero-day Exchange Server vulnerabilities.

January 5: A DEVCORE cybersecurity researcher finds 2 out of 4 vulnerabilities, and reports them to Microsoft. At the same time said 'This could be the most serious RCE I have ever reported'.

January 6: The first four zero-day vulnerabilities exploited

January: Dubex has also reported suspicious activity on Microsoft Exchange servers.

March 2: Microsoft releases patches to address four critical vulnerabilities of Exchange Server. At the same time, it is acknowledged that the vulnerabilities are actively exploited in "targeted attacks".

March 12: Microsoft launches an in-depth investigation to determine if hackers have the credentials needed to gain access to Microsoft partners' Exchange Server. .

March 10: Proof-of-Concept (PoC) attack code has been pushed to GitHub, after which GitHub deletes it.

March 14: New PoC code is released by another researcher, described as a method of bringing Exchange server exploits down to "script-kiddie" level.

It is suspected that the hacker groups possessed the PoC code that Microsoft shared with antivirus partners under the Microsoft Active Protections Program (Mapp).

Although fixes have been issued, the extent of potential Exchange Server intrusion is dependent on the speed at which the patches are received and applied from the enterprise. Therefore, the estimated number of victims will continue to increase.

Information about the vulnerabilities on Exchange Server

These critical vulnerabilities, collectively known as ProxyLogon, affect Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019. However, Exchange Online is not affected. The specific list is as follows:

1. **CVE-2021-26855** : **Server-side** request spoofing vulnerability (SSRF) allows attackers to send arbitrary HTTP requests and authenticate as Exchange servers
2. **CVE-2021-26857** : Vulnerability in Unified Messaging service, allowing attackers to execute arbitrary code
3. **CVE-2021-26858** : Exchange file logging vulnerability, attacker can optionally write to any path on server.
4. **CVE-2021-27065** : Exchange file logging vulnerability, an attacker can optionally write to any path on the server.

If used in a chain of attacks, all of these vulnerabilities can lead to remote code execution (RCE), server hijacking, backdoors, data theft, and the ability to further deploy. malware.

In short, Microsoft says attackers can securely access Exchange Server through these errors or stolen credentials. And then, they can create a web shell to take over the system and execute commands remotely.

> 'These vulnerabilities are used as part of the attack chain. The initial attack required the ability to create an untrusted connection to the Exchange server port 443. This can be countered either by restricting temporary connections or by setting up a VPN to separate the Exchange server from. external accesses.
>
> Using this mitigation will only provide protection from the initial part of the attack. Other parts of the chain could be triggered if an attacker already had access or could persuade (trick) the system administrator to run a malicious file '.

Responsible object

According to Microsoft, when it comes to tracing attacks that use zero-day vulnerabilities, it is highly likely that they were carried out by Hafnium, a highly skilled and sophisticated APT hacker group.

Hafnium uses VPS located in the US to try to conceal its true location. People previously targeted by this group include consulting organizations, nonprofits, defense contractors, and research organizations.

On March 10, ESET reported that 10 APT groups had been involved in attacks exploiting Exchange Server vulnerabilities, including LuckyMouse, Tick, Winnti Group and Calypso.

Infulence level

According to cybersecurity expert Brian Krebs, about 30,000 organizations in the US have been hacked to date. Bloomberg estimates bring this number to nearly 60,000, as of March 8. While Palo Alto Networks claims there are at least 125,000 servers that are not patched worldwide.

In its March 5 update, Microsoft said the company "continues to see an increasing abuse of vulnerabilities in attacks that target unpatched systems by multiple external malicious agents. Hafnium ".

From March 11 to March 15, Check Point Research said attack attempts have increased by 10 times based on data gathered during these days. The US, Germany and UK are the most targeted countries. Government and military targets accounted for 23% of the total attack effort, followed by manufacturing, financial services and software vendors.

In a situation reminiscent of the 2017 WannaCry ransomware outbreak, on March 12, Microsoft said a ransomware variant called DearCry is leveraging vulnerabilities to deploy ransomware on vulnerable Exchange servers. .

Solution to respond to vulnerabilities on Exchange Server

Microsoft urges IT administrators and companies using Exchange Server around the world to apply security fixes immediately. Also publishes a script on GitHub for IT administrators to run that includes intrusion indicators (IOCs) associated with four vulnerabilities. The IoC is listed separately here.

In addition, companies also need to actively strengthen surveillance and be ready to deal with signs of network exploitation and attacks. For organizations with technical personnel, good can test to penetrate the system through the serious security holes mentioned above.