











Exchange Server 2019 Vulnerability – Exploited by Hackers – 3rd March 2021

I am running hybrid exchange 2019 within the lab. I wanted to take necessary precaution to protect mail server. I did the following to make sure the server was not compromised by the hackers.

I am using various PowerShell scripts and commands to test the server. Here are the details

Name	Date modified	Type
 MSERT.exe	09-Mar-2021 10:07 AM	Application
 ZeroDayCheckScript.ps1	06-Mar-2021 2:25 PM	Windows PowerShell Script
 HealthCheck-EX2019-20210305202200.txt	05-Mar-2021 8:23 PM	Text Document
 HealthCheck-EX2019-20210305202200.xml	05-Mar-2021 8:23 PM	XML Document
 HealthChecker.ps1	05-Mar-2021 8:21 PM	Windows PowerShell Script
 http-vuln-cve2021-26855.nse	05-Mar-2021 8:00 PM	NSE File
 README.md	05-Mar-2021 7:26 PM	MD File
 BackendCookieMitigation.ps1	05-Mar-2021 7:25 PM	Windows PowerShell Script
 Test-ProxyLogon.ps1	05-Mar-2021 7:25 PM	Windows PowerShell Script
 detect_webshells.ps1	09-Mar-2021 3:27 ...	Windows PowerS... 5 KB

```
Administrator: Windows PowerShell
PS C:\Users\Administrator\RAJLAN\Documents\exchange_webshell_detection-main> dir

Directory: C:\Users\Administrator\RAJLAN\Documents\exchange_webshell_detection-main

Mode                LastWriteTime         Length Name
----                -
-a-----         09-Mar-2021  3:27 AM           4943 detect_webshells.ps1
-a-----         09-Mar-2021  3:27 AM           3518 Readme.md

PS C:\Users\Administrator\RAJLAN\Documents\exchange_webshell_detection-main> .\detect_webshells.ps1
No webshells found, but they might have been removed or attackers might have used other persistence techniques
PS C:\Users\Administrator\RAJLAN\Documents\exchange_webshell_detection-main> get-childitem -path c: -filter *.js -recurse -erroraction silentlycontinue | ?{($_.lastwritetime -gt (get-date).AddDays(-30))}
PS C:\Users\Administrator\RAJLAN\Documents\exchange_webshell_detection-main> get-childitem -path c: -filter *.aspx -recurse -erroraction silentlycontinue | ?{($_.lastwritetime -gt (get-date).AddDays(-30))}
PS C:\Users\Administrator\RAJLAN\Documents\exchange_webshell_detection-main> Import-Csv -Path (get-childitem -recurse -Path "$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\HttpProxy" -Filter "*.log").FullName
| Where-Object { $_.AuthenticatedUser -eq "" -and $_.AnchorMailbox -like 'ServerInfo~*/' } | select DateTime, AnchorMailbox
PS C:\Users\Administrator\RAJLAN\Documents\exchange_webshell_detection-main>
```

Import-Csv -Path (Get-ChildItem -Recurse -Path "\$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\HttpProxy" -Filter "*.log").FullName | Where-Object { \$_.AuthenticatedUser -eq "" -and \$_.AnchorMailbox -like 'ServerInfo~*/' } | select DateTime, AnchorMailbox

Get-childitem -path c: -filter *.js -recurse -erroraction silentlycontinue | ?{(\$_.lastwritetime -gt (get-date).AddDays(-30))}

Get-childitem -path c: -filter *.aspx -recurse -erroraction silentlycontinue | ?{(\$_.lastwritetime -gt (get-date).AddDays(-30))}

I did install these patches as well.

Update history

✓ Quality Updates (50)

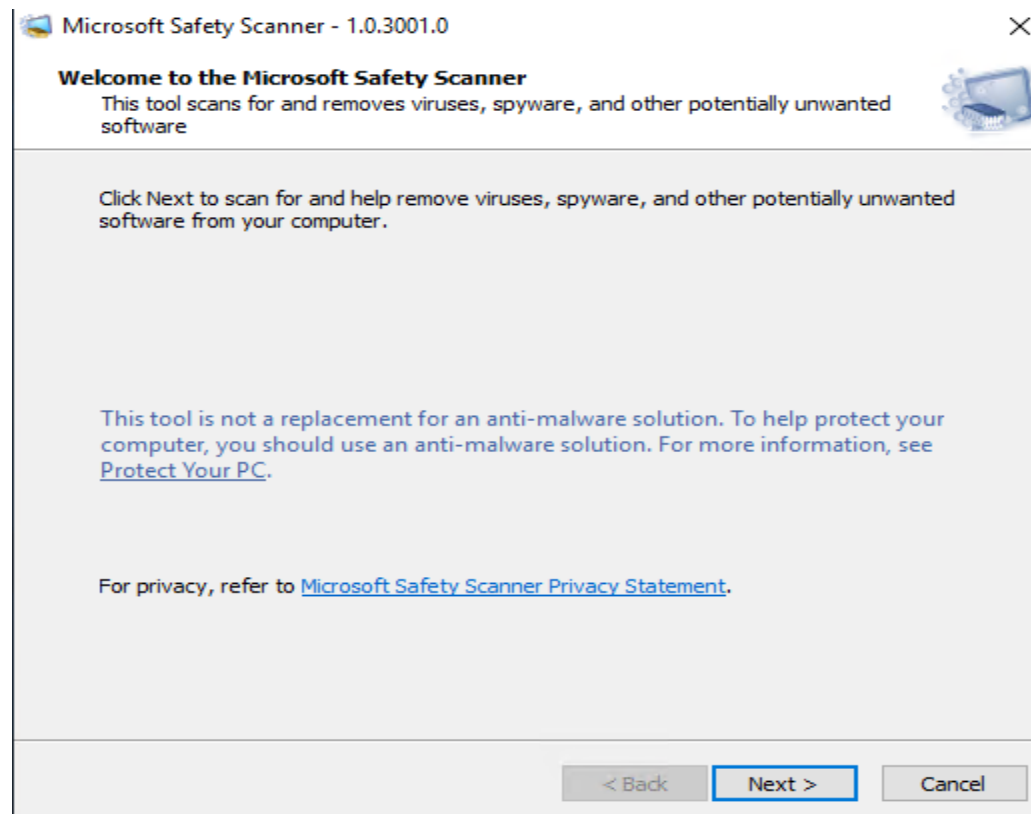
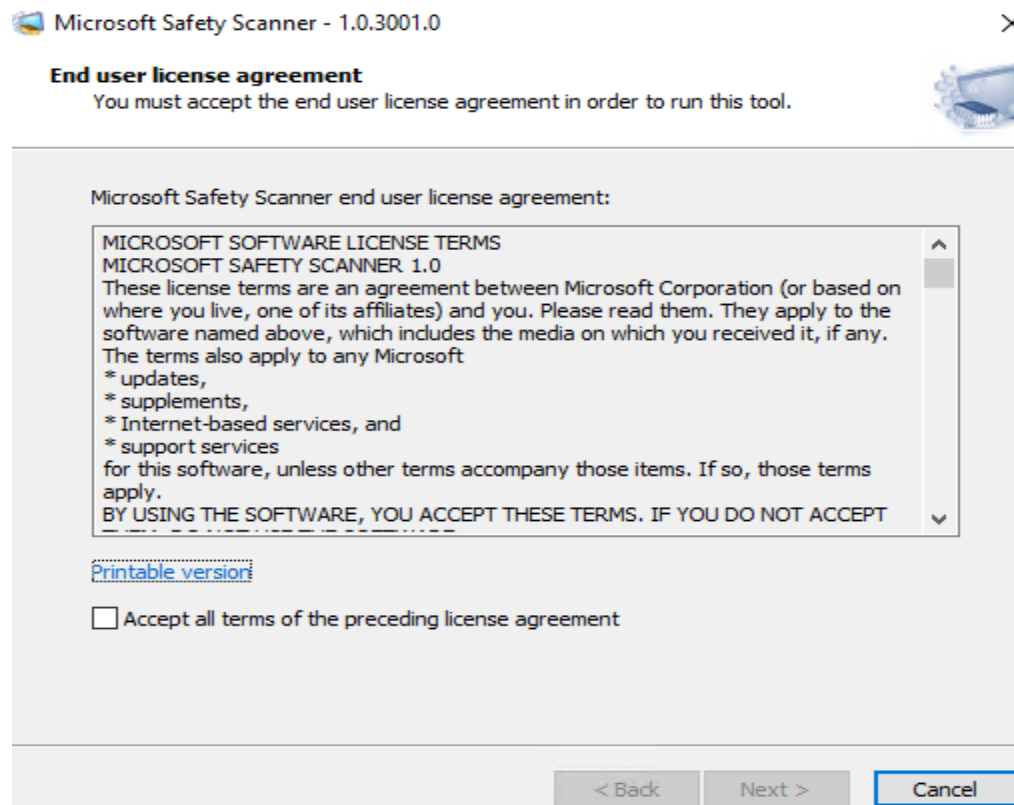
2021-02 Cumulative Update Preview for Windows Server 2019 (1809) for x64-based Systems (KB4601383)

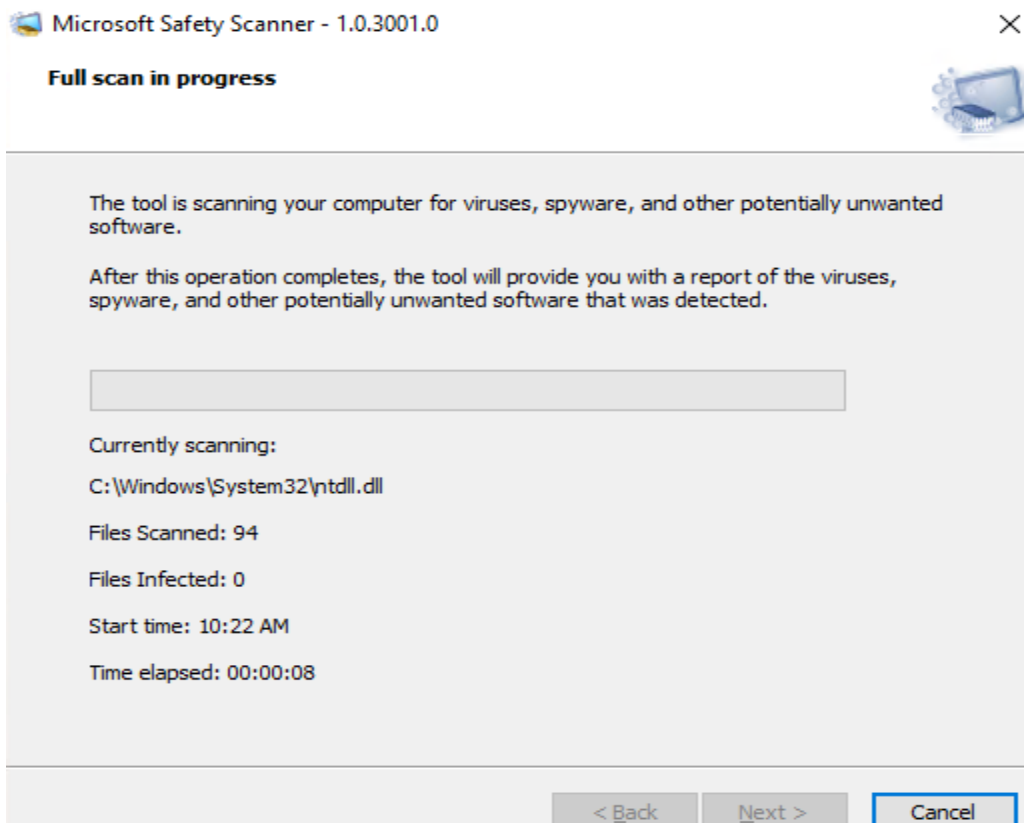
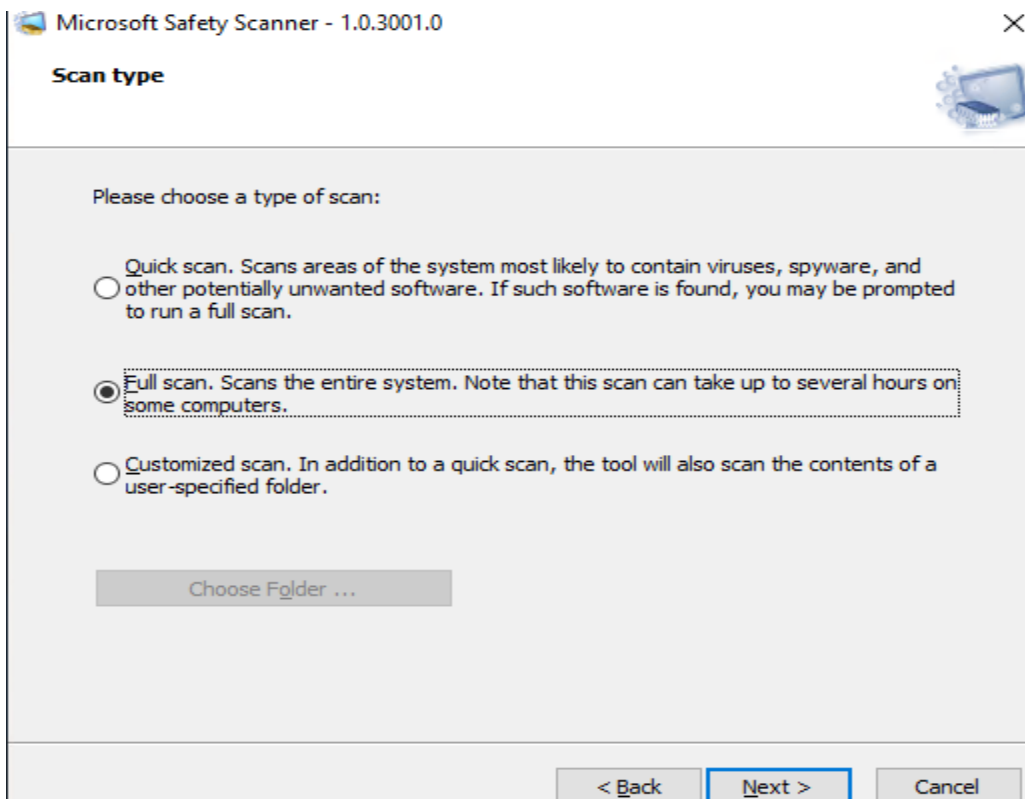
Successfully installed on 05-Mar-2021

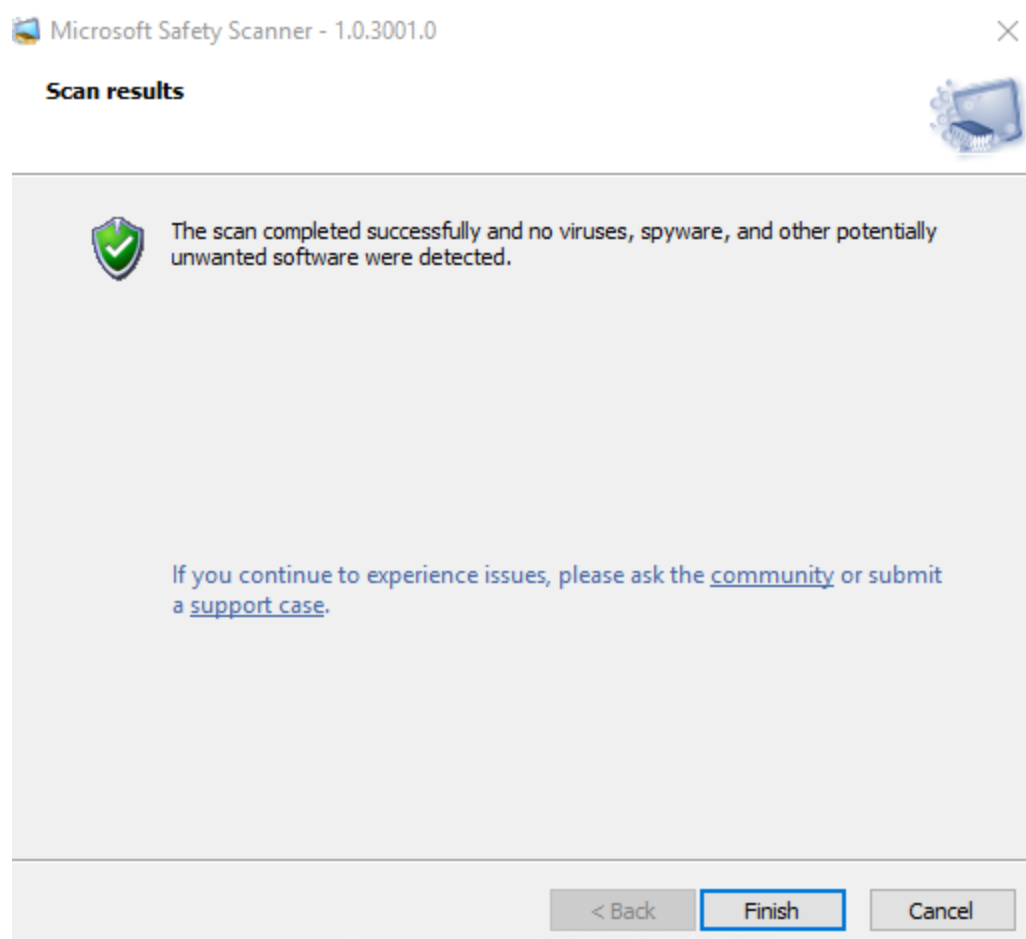
Security Update For Exchange Server 2019 CU8 (KB5000871)

Successfully installed on 04-Mar-2021

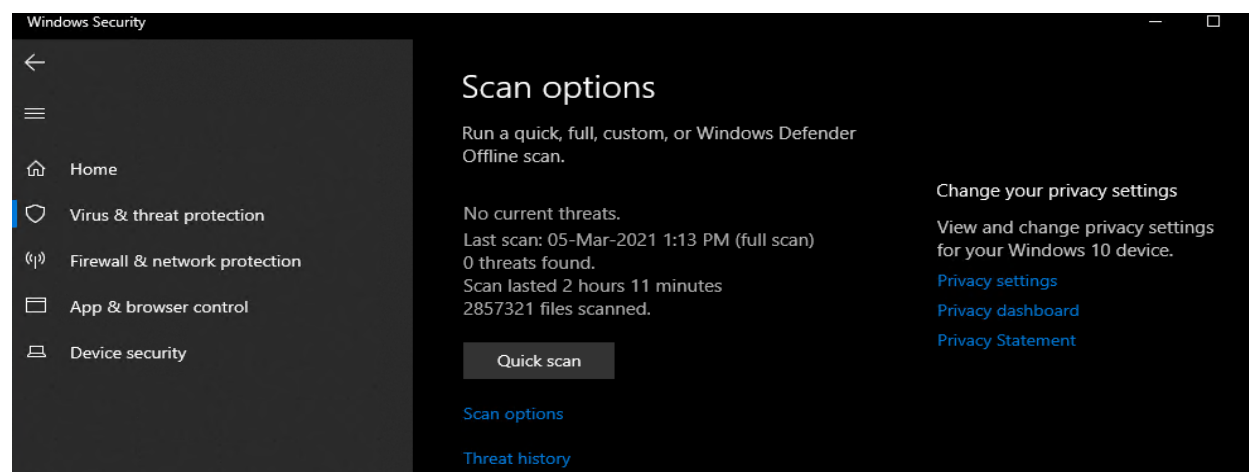
So far everything is looking good for me. I am running MSERT tool as well for extra precaution.







I also performed full scan using Windows Defender for extra protection.



Now, I am happy the mail server is not compromised and hackers did not penetrate the mail server.

Thanks

Ram Lan
9th Mar 2021

This picture below, I copied from Microsoft site for eash reference on how to protect mail server.

