






# 02 March 2021 – Exchange Server Security Update

Last updated: 17-March-2021  
Version 1.2.71



# Objectives

-  Present the different actions/workflow of your infrastructure updates based on the version currently installed
-  How to know if you have been compromised
-  How to remediate if you have been compromised

Following the Security "Out of Band" updates publication on the 2nd of March 2021, our purpose is to allow you to proceed with the update as soon as possible:

[Released: March 2021 Exchange Server Security Updates - Microsoft Tech Community](#)

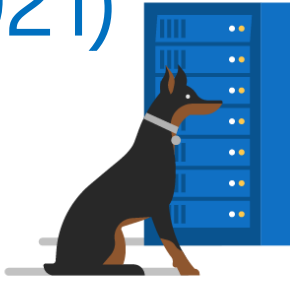
NEW! [Security Updates for older Cumulative Updates of Exchange Server](#)

NEW! [Guidance for responders: Investigating and remediating on-premises Exchange Server vulnerabilities – Microsoft Security Response Center](#)

# Glossary

- SP = Service Pack
- RU = Rollup Update
- CU = Cumulative Update
- SU = Security Update
- OOB = Out Of Band
- AD = Active Directory
- KB = Knowledge Base

# Out-of-band update for Exchange Server (March 2, 2021)



## Only on-premises Exchange Server installations are affected, Exchange Online is not

If you have a hybrid configuration, then you have at least one Exchange on-premises server, and it needs to be updated

- Exchange Server 2013
- Exchange Server 2016
- Exchange Server 2019
- Exchange Server 2010 - this product is not vulnerable to the attack chain, but an update has been released for defense in depth purposes

Attacks are targeting the following versions: Exchange 2013/2016/2019 (any currently available CU)

## How critical is this update?

Very – install the update now!

Prioritize installation on Internet-exposed/Internet-facing Exchange servers (e.g., servers publishing OWA and ECP), then install the update on all remaining Exchange servers in your environment.

Microsoft recommends applying the update to your infrastructure to remediate the vulnerability, then search for indicators of compromise.

My Exchange Server is supported by original March 2021 security releases:

- Exchange Server 2010 SP 3 or later
- Exchange Server 2013 CU 23
- Exchange Server 2016 CU 19 or CU 18
- Exchange Server 2019 CU 8 or CU 7

Install March 2021 Security Updates

Exchange is up to date

Updated for all known security vulnerabilities including March 2021

My Exchange Server is NOT supported by original March 2021 security releases.

I am getting my environment supported to install security updates.

Install latest CU / RU

Install March 2021 Security Updates

Exchange is up to date

Updated for all known security vulnerabilities including March 2021

New path

My Exchange Server is NOT supported by original March 2021 security releases.

I am *not able* to get my environment updated to install security updates.

Install released March 2021 Security Updates for older CUs

Exchange is not up to date

Updated for March 2021 security vulnerabilities *only*

Install latest CU and SUs

Exchange is up to date

Updated for all known security vulnerabilities including March 2021

# My server is Exchange Server 2019 CU8

**RECOMMENDED** - You can install the new CU9 with Security Updates included

See Article - [Cumulative Update 9 for Exchange Server 2019 \(microsoft.com\)](https://microsoft.com/support/kbkb4602570)

Customers should install Exchange Server 2019 Cumulative Update 9 ([KB4602570](https://support.microsoft.com/kb/kb4602570)), [VLSC Download](#) as follows:

1. Put the server into [Maintenance mode](#)
  - If you don't currently have a written procedure, you can use the following: [Performing maintenance on DAG members](#)
2. Reboot prior to installation.
3. Proceed with CU installation
4. Reboot after the installation, even if not prompted
5. Exit [Maintenance mode](#)
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

# My server is Exchange Server 2019 CU8 or CU7

## You can install the SU

Customers should install [KB5000871](#) (CU8) or [KB5000871](#) (CU7) SU as follows:

1. Put the server into [Maintenance mode](#)
  - If you don't currently have a written procedure, you can use the following: [Performing maintenance on DAG members](#)
2. Reboot prior to installation.
3. Proceed with SU installation via elevated/admin cmd prompt (see *Known Issues* section)
4. Reboot after the installation, even if not prompted
5. Exit [Maintenance mode](#)
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

# My server is Exchange Server 2019 CU7

## Server is on CU7 and you already planned to install CU8

If you were already planning to install CU8, do not wait until you are on CU8 to install the SU.

- Install the SU **now** (using the steps on the previous slide)
  - Later, apply CU8 as appropriate following the steps below. Please note that you will need to **reapply the SU for CU8 afterwards!**
1. Update AD using [Exchange Server 2019 CU8](#), as follows:
    - Setup.exe /PrepareSchema, etc ..... [Additional help here](#)
    - Setup.exe /PrepareAD, etc ..... [Additional help here](#)
  2. Apply CU8, which means:
    - Put the server into [Maintenance mode](#)
    - Reboot the server
    - Backup your customizations (OWA: themes, logo; Other configurations: limited number of OU; Everything that hasn't been done using a PowerShell command...)
    - Install CU8 **via elevated/admin cmd prompt** (see *known issues section*)
    - Reboot after the installation
  3. Then, reapply the [KB5000871](#) SU, which means:
    - The server is still in [Maintenance mode](#)
    - Proceed with SU installation **via elevated/admin cmd prompt** (see *Known Issues* section)
    - Reboot after the installation, even if not prompted
    - Restore your previously saved customizations
  4. Exit maintenance mode based on your [usual procedure](#)
  5. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

# My server is Exchange Server 2019 CU7 or older

## Recommended steps to update the Exchange server to CU9

1. Verify .NET Framework version using this [procedure](#)
  - If it is not 4.8, update it, which means:
    - Put server into [Maintenance mode](#)
    - Stop all Exchange Services
    - .NET Framework 4.8 installation **via elevated/admin cmd prompt**
    - Reboot after the installation
2. Update AD using [Exchange Server 2019 CU9](#), as follows:
  - Setup.exe /PrepareSchema, etc ..... [Additional help here](#)
  - Setup.exe /PrepareAD, etc ..... [Additional help here](#)
3. Apply CU9 as follows:
  - The server is still in [Maintenance mode](#)
  - Backup all customizations (OWA: themes, logo; Other configurations: limited number of OU; Everything that hasn't been done using a PowerShell command...)
  - Install CU9 **via elevated/admin cmd prompt** (see *Known Issues* section)
  - Reboot after the installation
4. Exit maintenance mode based on your [usual procedure](#)
5. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

### Exchange 2019

.NET Framework version	CU8 to CU4	CU3, CU2	CU1, RTM
4.8	Supported	Supported	Not supported
4.7.2	Not supported	Supported	Supported

# My server is Exchange Server 2019 CU6,5,4,3 or RTM

You can install the SU for some older CUs as a temporary measure

You could install [KB5000871](#) (CU6) or [KB5000871](#) (CU5) or [KB5000871](#) (CU4) or [KB5000871](#) (CU3) or [KB5000871](#) (CU2) or [KB5000871](#) (CU1) or [KB5000871](#) (RTM) SU as a temporary measure released Mar 12 (PST), 2021.

**Note:** Installing these updates does not mean an unsupported CU is now supported.

1. Put the server into [Maintenance mode](#)
  - If you don't currently have a written procedure, you can use the following: [Performing maintenance on DAG members](#)
2. Reboot prior to installation.
3. Proceed with SU installation via elevated/admin cmd prompt (see *Known Issues* section)
4. Reboot after the installation, even if not prompted
5. Exit [Maintenance mode](#)
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)
7. Update to latest CU as soon as it is available.

# My server is Exchange Server 2016 CU19

**RECOMMENDED** - You can install the new CU20 with Security Updates included

See Article - [Cumulative Update 20 for Exchange Server 2016 \(microsoft.com\)](#)

Customers should install Exchange Server 2016 Cumulative Update 20 ([KB4602569](#)), [Download](#), [UM Lang Packs](#) as follows:

1. Put the server into [Maintenance mode](#)
  - If you don't currently have a written procedure, you can use the following: [Performing maintenance on DAG members](#)
2. Reboot prior to installation.
3. Proceed with CU installation
4. Reboot after the installation, even if not prompted
5. Exit [Maintenance mode](#)
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

# My server is Exchange Server 2016 CU19 or CU18

## You can install the SU

You have to install the [KB5000871](#) (CU18) or [KB5000871](#) (CU19) or SU as follows:

1. Put the server into [Maintenance mode](#)
  - If you don't currently have a written procedure, you can use the following: [Performing maintenance on DAG members](#)
2. Reboot the server
3. Proceed with SU installation via elevated/admin cmd prompt (see *Known Issues* section)
4. Reboot after the installation, even if not prompted
5. Exit [Maintenance mode](#)
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

# My server is Exchange Server 2016 CU18

## Your server is on CU18 and you already planned to install CU19

If you were planning to install CU19, do not wait until you are on CU19 to install the SU

- Install the SU **now** (using the steps on the previous slide)
  - Later, apply CU19 as appropriate following the steps below. Please note that you will need to **reapply the SU for CU19 afterwards!**
1. Update AD update [Exchange Server 2016 CU19](#), as follows:
    - Setup.exe /PrepareSchema, etc ..... [Additional help here](#)
    - Setup.exe /PrepareAD, etc ..... [Additional help here](#)
  2. Apply CU19 as follows:
    - Put the server into [Maintenance mode](#)
    - Reboot the server
    - Backup your customizations (OWA: themes, logo; Other configurations: limited number of OU; Everything that hasn't been done using a PowerShell command...)
    - Install CU19 **via elevated/admin cmd prompt** (see *Known Issues* section)
    - Reboot after the installation
  3. **Reapply** the [KB5000871](#) SU as follows:
    - The server is still in [Maintenance mode](#)
    - Proceed with SU installation **via elevated/admin cmd prompt** (see *Known Issues* section)
    - Reboot after the installation, even if not prompted
    - Restore your previously saved customizations
  4. Exit maintenance mode based on your [usual procedure](#)
  5. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

# My server is Exchange Server 2016 CU18 or older

## Recommended steps to update the Exchange server to CU20

1. Verify version of .NET Framework using this [procedure](#)
  - If it is not 4.8, update it as follows:
    - Put the server into [Maintenance mode](#)
    - Stop all Exchange Services
    - Install .NET Framework 4.8 [via elevated/admin cmd prompt](#)
    - Reboot after the installation
2. Update AD using [Exchange Server 2016 CU20](#), as follows:
  - Setup.exe /PrepareSchema, etc ..... [Additional help here](#)
  - Setup.exe /PrepareAD, etc ..... [Additional help here](#)
3. Apply CU20 as follows:
  - The server is still in [Maintenance mode](#)
  - Backup all customizations (OWA: themes, logo; Other configurations: limited number of OU; Everything that hasn't been done using a PowerShell command...)
  - Install CU20 [via elevated/admin cmd prompt](#) (see *Known Issues* section)
  - Reboot after the installation
4. Exit maintenance mode based on your [usual procedure](#)
5. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

Exchange 2016

.NET Framework version	CU19 to CU15	CU14, CU13	CU12, CU11	CU10	CU9, CU8	CU7, CU6, CU5	CU4, CU3
4.8	Supported	Supported	Not supported	Not supported	Not supported	Not supported	Not supported
4.7.2	Not supported	Supported	Supported	Not supported	Not supported	Not supported	Not supported
4.7.1	Not supported	Not supported	Supported	Supported	Supported	Not supported	Not supported
4.6.2	Not supported	Not supported	Not supported	Not supported	Supported	Supported	Supported
4.6.1*	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported
4.5.2	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported

# My server is Exchange Server 2016 CU8,9,10,11,12,13,14,15,16 or 17

You can install the SU for some older CUs as a temporary measure

You could install [KB5000871](#) (CU8) or [KB5000871](#) (CU9) or [KB5000871](#) (CU10) or [KB5000871](#) (CU11) or [KB5000871](#) (CU12) [KB5000871](#) (CU13) or [KB5000871](#) (CU14) [KB5000871](#) (CU15) [KB5000871](#) (CU16) or [KB5000871](#) (CU17) SU as a temporary measure released Mar 12 (PST), 2021

**Note:** Installing these updates does not mean an unsupported CU is now supported.

1. Put the server into [Maintenance mode](#)
  - If you don't currently have a written procedure, you can use the following: [Performing maintenance on DAG members](#)
2. Reboot prior to installation.
3. Proceed with SU installation via elevated/admin cmd prompt (see *Known Issues* section)
4. Reboot after the installation, even if not prompted
5. Exit [Maintenance mode](#)
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)
7. Update to latest CU as soon as it is available.

# My server is Exchange Server 2013 CU23

## You can install the SU

Install the [KB5000871](#) SU as follows:

1. Put the server into [Maintenance mode](#)
  - If you don't currently have a written procedure, you can use the following: [Performing maintenance on DAG members](#)
2. Reboot the server
3. Proceed with SU installation via elevated/admin cmd prompt (see *Known Issues* section)
4. Reboot after the installation, even if not prompted
5. Exit [Maintenance mode](#)
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

# My server is Exchange Server 2013 CU22 or older

## Recommended steps to update the Exchange server before applying the SU

1. Verify .NET Framework version using this [procedure](#)
  - If it is not 4.8, update it, which means:
    - Put the server into [Maintenance mode](#)
    - Stop all Exchange Services
    - Install .NET Framework 4.8 via elevated/admin cmd prompt
    - Reboot after the installation
2. Update AD using [Exchange Server 2013 CU23](#):
  - Setup.exe /PrepareSchema, etc ..... [Additional help here](#)
  - Setup.exe /PrepareAD, etc ..... [Additional help here](#)
3. Apply CU23, which means:
  - The server is still in [Maintenance mode](#)
  - Backup all customizations (OWA: themes, logo; Other configurations: limited number of OU; Everything that hasn't been done using a PowerShell command...)
  - Install CU23 via elevated/admin cmd prompt (see *Known Issues* section)
  - Reboot after the installation
4. Apply the [KB5000871](#) SU, which means:
  - The server is still in [Maintenance mode](#)
  - Proceed with SU installation via elevated/admin cmd prompt (see *Known Issues* section)
  - Reboot after the installation, even if not prompted
  - Restore your previously saved customizations
5. Exit maintenance mode based on your [usual procedure](#)
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

Exchange 2013

.NET Framework version	CU23	CU21, CU22	CU19, CU20	CU16, CU17, CU18	CU15	CU13, CU14
4.8	Supported	Not supported	Not supported	Not supported	Not supported	Not supported
4.7.2	Supported	Supported	Not supported	Not supported	Not supported	Not supported
4.7.1	Not supported	Supported	Supported	Not supported	Not supported	Not supported
4.6.2	Not supported	Not supported	Supported	Supported	Supported	Not supported
4.6.1*	Not supported	Not supported	Not supported	Not supported	Supported	Supported
4.5.2	Not supported	Not supported	Not supported	Not supported	Supported	Supported

# My server is Exchange Server 2013 CU21 or 22

You can install the SU for some older CUs as a temporary measure

You could install [KB5000871](#) (CU21) or [KB5000871](#) (CU22) SU as a temporary measure released Mar 10 (PST), 2021

**Note: Installing these updates does not mean an unsupported CU is now supported.**

1. Put the server into [Maintenance mode](#)
  - If you don't currently have a written procedure, you can use the following: [Performing maintenance on DAG members](#)
2. Reboot prior to installation.
3. Proceed with SU installation via elevated/admin cmd prompt (see *Known Issues* section)
4. Reboot after the installation, even if not prompted
5. Exit [Maintenance mode](#)
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)
7. Update to latest CU as soon as it is available.

# My server is Exchange Server 2013 SP1 (CU4)

You can install the SU on Exchange 2013 SP1 (CU4) as a temporary measure

You could install [KB5000871](#) (2013 SP1 CU4) SU as a temporary measure released Mar 16 (PST), 2021

**Note: Installing this update does not mean this unsupported CU is now supported.**

1. Put the server into [Maintenance mode](#)
  - If you don't currently have a written procedure, you can use the following: [Performing maintenance on DAG members](#)
2. Reboot prior to installation.
3. Proceed with SU installation via elevated/admin cmd prompt (see *Known Issues* section)
4. Reboot after the installation, even if not prompted
5. Exit [Maintenance mode](#)
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)
7. Update to latest CU as soon as it is available.

# My server is Exchange Server 2010 RU31

## You can install RU32

Install the [KB5000978](#) RU32 (defense in depth update), which means:

1. Put the server into maintenance mode
  - If you don't currently have the written procedure, you can use the following one: [Performing maintenance on DAG members](#)
2. Reboot the server
3. Proceed with RU32 installation via elevated/admin cmd prompt (see *Known Issues* section)
4. Reboot after the installation, even if not prompted
5. Exit maintenance mode
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

# My server is Exchange Server 2010 SP3 (no RU)

or any post-SP3 RU (1-30)

## You can install RU32

You have to install the [KB500978](#) RU32 (defense in depth update), which means:

1. Put the server into maintenance mode
  - If you don't currently have the written procedure, you can use the following: [Installing Update Rollups on Database Availability Group Members: Exchange 2010 Help | Microsoft Docs](#)
2. Reboot the server
3. Proceed with RU32 installation via elevated/admin cmd prompt (see *Known Issues* section)
4. Reboot after the installation, even if not prompted
5. Exit maintenance mode
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

# My server is Exchange Server 2010 SP2 or older

## You need to update Exchange server before applying the SP3 RU32

1. Verify .NET Framework version using this [procedure](#)
  - If it is not 4.5, update it as follows:
    - Put the server into [Maintenance mode](#)
    - Stop all Exchange Services
    - Install .NET Framework 4.5 [via elevated/admin cmd prompt](#)
    - Reboot after the installation
2. Update AD using [Exchange Server 2010 SP3](#) as follows:
  - Setup.exe /PrepareSchema, etc ..... [Additional help here](#)
  - Setup.exe /PrepareAD, etc ..... [Additional help here](#)
3. Apply Exchange Server SP3 as follows:
  - The server is still in maintenance mode
  - Backup all customizations (OWA: themes, logo; Other configurations: limited number of OU; Everything that hasn't been done using a PowerShell command...)
  - SP3 installation [via elevated/admin cmd prompt](#) (see *Known Issues* section)
  - Reboot after the installation
4. Apply the [KB5000978](#) RU32 as follows:
  - The server is still in maintenance mode
  - Proceed with RU installation [via elevated/admin cmd prompt](#) (see *Known Issues* section)
  - Reboot after the installation, even if not prompted
  - Restore your previously saved customizations
5. Exit maintenance mode based on your [usual procedure](#)
6. Verify all additional applications connecting to Exchange (Backup, Archiving, Monitoring, ...)

### Exchange 2010 SP3

.NET Framework version	Exchange 2010 SP3
.NET Framework 4.5	Supported <sup>1,2</sup>
.NET Framework 4.0	Supported <sup>1,2</sup>
.NET Framework 3.5 SP1	Supported
.NET Framework 3.5	Supported <sup>1</sup>

# Known Issues

# Frequently encountered errors

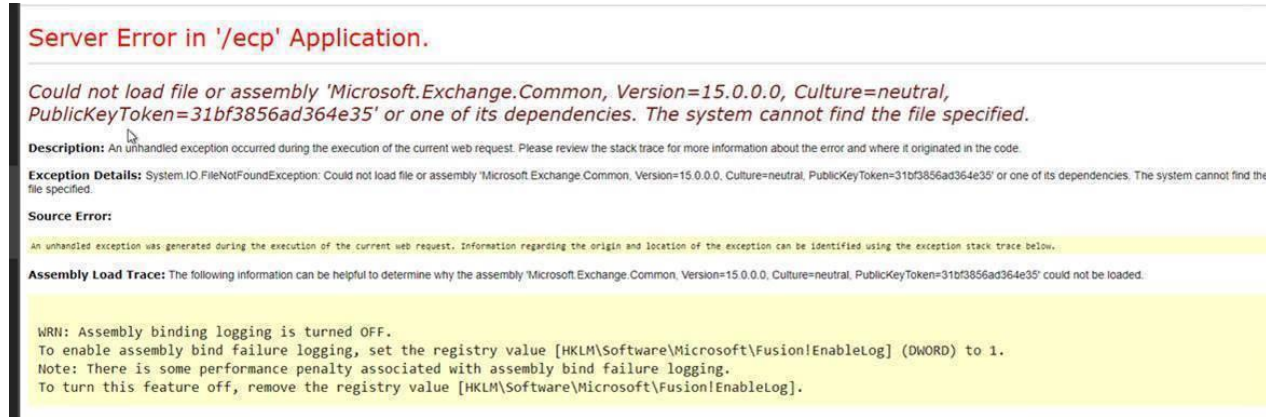
## Cannot access ECP post-installation

Likely reason: Security Update not installed via elevated/admin cmd prompt

→ Solution: Reinstall the update via elevated/admin cmd prompt

→ And/or run the UpdateCAS.ps1 script located in C:\Program Files\Microsoft\Exchange Server\V15\Bin

More information can be found at <https://aka.ms/exupdatefaq>



## PrepareAD generated an error:

Run it again from an **elevated cmd prompt** or PowerShell instance

→ No issues with running it several times

```
0:\>Setup.EXE /IAcceptExchangeServerLicenseTerms /PrepareSchema
Microsoft Exchange Server 2016 Cumulative Update 19 Unattended Setup

Copying Files...
File copy complete. Setup will now collect additional information needed for installation.

Performing Microsoft Exchange Server Prerequisite Check
  Prerequisite Analysis
Configuring Microsoft Exchange Server
  Extending Active Directory schema
  88%
An unexpected error has occurred and a Watson dump is being generated: Exception has been thrown by the target of an
invocation.

Task module "AutoReportProgressModule.ReportProgressCompleted" fails with exception
"Exception has been thrown by the target of an invocation.". This module is skipped. Task
execution result should not be affected.
Exception has been thrown by the target of an invocation.

The Exchange Server setup operation didn't complete. More details can be found in ExchangeSetup.log
located in the <SystemDrive>\ExchangeSetupLogs folder.
```

# Frequently encountered errors

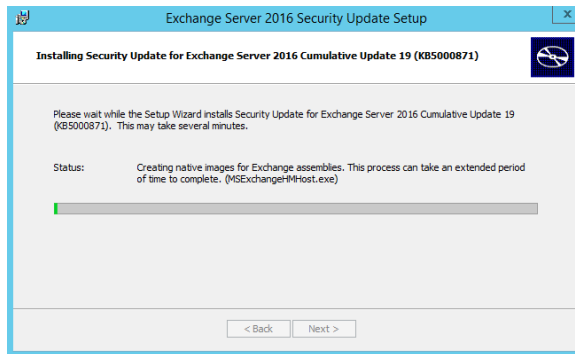
## Issues after installation of Exchange Server security updates:

More information can be found at [Issues due to Exchange Server security updates - Exchange | Microsoft Docs](#)

# Frequently encountered errors

## The Security Update installation is taking a long time

If your Exchange server doesn't have access to the Internet, the SU installation will take a lot of time, especially during this step:

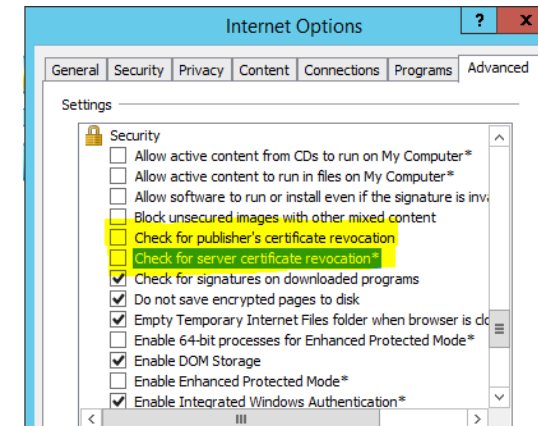


→ Solution: Deactivate the 2 CRL control options :

To access the settings there are two options

- Option 1: In the Server's default web browser, Select "Internet Options"
- Option 2: Go to the Control panel and Select "Internet options"
- Once in Options, navigate to Advanced and de-select certificate revocation checkboxes

→ **Warning:** Do not forget to reactivate options once the installation is complete!



# Investigation & Remediation

# Microsoft Defender technologies (Slide 1)

- Microsoft is aware of active attacks utilizing the vulnerabilities that were addressed in the March 2<sup>nd</sup> out-of-band release for Exchange Server. The observed attacks are by multiple actors with multiple tools and objectives.
- Customers are strongly advised to deploy the updates into their environments as soon as possible.
- This remains a dynamic and quickly changing threat environment.
- Microsoft Defender antivirus helps protect against the known malware in build version **1.331.2471.0** or higher.
- Microsoft Defender for Endpoint helps protect against attack behaviours observed in this post-compromise attack.

# Microsoft Defender technologies (Slide 2)

## Solutions

- Microsoft's strong recommendation is that customers upgrade their on-premises Exchange environments and install the Security Update.
- Microsoft Defender for Endpoint and Microsoft Defender antivirus provide detection for the known behaviours and malware. Customers should keep antimalware products up-to-date. Customers utilizing automatic updates do not need to take additional action to receive these protections. Enterprise customers managing updates should select the new detection build (**1.331.2471.0** or newer) and deploy it across their environments.

Detections Detection version 1.331.2471.0 or higher	
Microsoft Defender antivirus provides detections for threat components under the following detection:	Additional secondary stage attacks (not comprehensive) have been observed under the following threat families:
<ul style="list-style-type: none"><li>• Exploit:Script/Exmann.A!dha</li><li>• Behavior:Win32/Exmann.A</li><li>• Behavior:Win32/Exmann.B</li><li>• Behavior:Win32/Exmann.C</li><li>• Behavior:Win32/Exmann.D</li><li>• Exploit:ASP/CVE-2021-27065</li></ul>	<ul style="list-style-type: none"><li>• Backdoor:JS/Webshell</li><li>• Trojan:JS/Chopper</li><li>• Backdoor:ASP/Chopper</li><li>• Behavior:Win32/DumpLsass</li><li>• Behavior:Win32/IISExchgDropWebshell</li><li>• Behavior:Win32/WebShellTerminal</li><li>• Trojan:Win32/CobaltLoader</li><li>• Trojan:BAT/CobaltLauncher</li></ul>

# Microsoft Defender technologies (Slide 3)

- Customers can also use the stand-alone tool called Microsoft Support Emergency Response Tool (MSERT) to help them remediate a server that is suspected to have been compromised.
- Information is available in the [Microsoft Exchange Server Vulnerabilities Mitigations – updated March 6, 2021](#) blog post, and the tool can be download from [here](#).

# Additional Information

## Microsoft Exchange Server Vulnerabilities Mitigations – updated March 6, 2021

Microsoft previously [blogged](#) our **strong recommendation that customers upgrade their on-premises Exchange environments to the latest supported version**. For customers that are not able to quickly apply updates, we are providing the following alternative mitigation techniques to help Microsoft Exchange customers who need more time to patch their deployments and are **willing to make risk and service function trade-offs**.

**These mitigations are not a remediation if your Exchange servers have already been compromised, nor are they full protection against attack**. We strongly recommend investigating your Exchange deployments using the hunting recommendations [here](#) to ensure that they have not been compromised. We recommend initiating an investigation in parallel with or after applying one of the following mitigation strategies.

This blog also contains a nmap script to help you discover vulnerable servers within your own infrastructure.

[Microsoft Exchange Server Vulnerabilities Mitigations – updated March 6, 2021 – Microsoft Security Response Center](#)

# Sources

Additional information can be found in the following links

- NEW! [Security Updates for older Cumulative Updates of Exchange Server](#)
- NEW! Exchange On-premises Mitigation Tool (EOMT) [CSS-Exchange/Security at main · microsoft/CSS-Exchange · GitHub](#)
- FAQ Microsoft : [Released: March 2021 Exchange Server Security Updates - Microsoft Tech Community](#)
- Attack explanations by Microsoft : [HAFNIUM targeting Exchange Servers with 0-day exploits - Microsoft Security](#)
- Exchange Server antivirus exclusions: [Running Windows antivirus software on Exchange servers | Microsoft Docs](#)
- Exchange .NET Framework Supportability Matrix: [Exchange Server supportability matrix | Microsoft Docs](#)
- CVE-2021-26412 : [CVE-2021-26412](#) *(not associated to known attacks)*
- CVE-2021-26854 : [CVE-2021-26854](#) *(not associated to known attacks)*
- CVE-2021-26855 : [CVE-2021-26855](#)
- CVE-2021-26857 : [CVE-2021-26857](#)
- CVE-2021-26858: [CVE-2021-26858](#)
- CVE-2021-27065: [CVE-2021-27065](#)
- CVE-2021-27078: [CVE-2021-27078](#) *(not associated to known attacks)*