Microsoft Exchange Server Vulnerabilities Mitigations – updated March 15, 2021

msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021

Update March 15, 2021: *If you have not yet patched, and have not applied the mitigations referenced below, a one-click tool, the Exchange On-premises Mitigation Tool is now our recommended path to mitigate until you can patch.*

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. **All the scripts and tools mentioned in this blog, along with guidance on using them can be found here:** https://github.com/microsoft/CSS-Exchange/blob/main/Security/

Customers should choose one of the following mitigation strategies based on your organization's priorities:

Recommended solution: ***Install the security patch***

- This method is the **only complete mitigation** and has no impact to functionality.
- The following has details on how to install the security update: https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901
- This will not evict an adversary who has already compromised a server.

Interim mitigations if unable to patch Exchange Server 2013, 2016, and 2019:

- Implement an IIS Re-Write Rule to filter malicious https requests
- Disable Unified Messaging (UM)
- Disable Exchange Control Panel (ECP) VDir
- Disable Offline Address Book (OAB) VDir

These mitigations can be applied or rolled back using the ExchangeMitigations.ps1 script described below and have some known impact to Exchange Server functionality. The mitigations are effective against the attacks we have seen so far in the wild but are not guaranteed to be complete mitigations for all possible exploitation of these vulnerabilities. This will not evict an adversary who has already compromised a server. ***This should only be used as a temporary mitigation until Exchange servers can be fully patched, and we recommend applying all of the mitigations at once.***

ExchangeMitigations.ps1

Overview

This script contains mitigations to help address the following vulnerabilities:

- CVE-2021-26855
- CVE-2021-26857
- CVE-2021-27065
- CVE-2021-26858

This script is to be executed via an elevated Exchange PowerShell Session or elevated Exchange Management Shell. Details for mitigations are below and additional information is on the aforementioned GitHub.

Backend Cookie Mitigation

Applies To: CVE-2021-26855

Description: This mitigation will filter https requests that contain malicious X-AnonResource-Backend and malformed X-BEResource cookies which were found to be used in the SSRF attacks in the wild. This will help with defense against the known patterns observed but not the SSRF as a whole.

Note: The IIS Rewrite rules will be removed after Exchange is upgraded and the mitigation will need to be reapplied if the security patch has not been installed.

Requirements: URL Rewrite Module

- For IIS 10 and higher URL Rewrite Module 2.1 is recommended, version 2.1 (x86 and x64) can be downloaded here:
  https://www.iis.net/downloads/microsoft/url-rewrite
- For IIS 8.5 and lower Rewrite Module 2.0 is recommended, version 2.0 can be downloaded here:
  - x86 – https://www.microsoft.com/en-us/download/details.aspx?id=5747
  - x64 – https://www.microsoft.com/en-us/download/details.aspx?id=7435

Impact: No **known** impact to Exchange functionality if URL Rewrite module is installed as recommended**.**

Installing URL Rewrite version 2.1 on IIS versions 8.5 and lower may cause IIS and Exchange to become unstable. If there is a mismatch between the URL Rewrite module and IIS version, ExchangeMitigations.ps1 will not apply the mitigation for CVE-2021-26855. You must uninstall the URL Rewrite module and reinstall the correct version.

Unified Messaging Mitigation

Applies To: CVE-2021-26857

Description: This mitigation will disable the Unified Message services in Exchange. Microsoft Exchange Managed Availability services are also disabled to prevent mitigation regression.

Impact: Unified Messaging/Voicemail outage when these services are disabled. The advanced monitoring capabilities of Exchange are also disabled, due to disabling Microsoft Exchange Managed Availability services.

ECP Application Pool Mitigation

Applies To: CVE-2021-27065 & CVE-2021-26858

Description: This mitigation will disable the Exchange Control Panel (ECP) Virtual Directory. Microsoft Exchange Managed Availability services are also disabled to prevent mitigation regression.

Impact: The Exchange Control Panel will no longer be available. All Exchange Administration can be done via Remote PowerShell while the Exchange Control Panel is disabled. The advanced monitoring capabilities of Exchange are also disabled, due to disabling Microsoft Exchange Managed Availability services.

OAB Application Pool Mitigation

Applies To: CVE-2021-27065 & CVE-2021-26858

Description: This mitigation disables the Offline Address Book (OAB) Application Pool and API. Microsoft Exchange Managed Availability services are also disabled to prevent mitigation regression.

Impact: OAB will be unavailable, including downloads of the Offline Address Book by Outlook clients. This may result in stale address book results in some scenarios and configurations. The advanced monitoring capabilities of Exchange are also disabled, due to disabling Microsoft Exchange Managed Availability services.

Additional hunting and investigation techniques

Nmap Script To Scan For CVE-2021-26855

Description: Detects whether the specified URL is vulnerable to the Exchange Server SSRF Vulnerability (CVE-2021-26855). This can be used to validate patch and mitigation state of exposed servers.

Test-ProxyLogon.Ps1

Description:

This script checks targeted exchange servers for signs of the proxy logon compromise. Proxy logon vulnerabilities are described in CVE-2021-26855, 26858, 26857, and 27065. This script is intended to be run via an elevated Exchange Management Shell.

Microsoft Support Emergency Response Tool (MSERT) to scan Microsoft Exchange Server

Microsoft Defender has included security intelligence updates to the latest version of the Microsoft Safety Scanner (MSERT.EXE) to detect and remediate the latest threats known to abuse the Exchange Server vulnerabilities disclosed on March 2, 2021. Administrators can use this tool for servers not protected by Microsoft Defender for Endpoint or where exclusions are configured for the recommended folders below.

To use the Microsoft Support Emergency Response Tool (MSERT) to scan the Microsoft Exchange Server locations for known indicators from adversaries:

1. Download MSERT from Microsoft Safety Scanner Download – Windows security. **Note:** In case you need to troubleshoot it, see How to troubleshoot an error when you run the Microsoft Safety Scanner.
2. Read and accept the **End user license agreement**, then click **Next**.
3. Read the **Microsoft Safety Scanner Privacy Statement**, then click **Next**.
4. Select whether you want to do full scan, or customized scan.

- **Full scan** – The most effective way to thoroughly scan every file on the device. It is the most effective option although it might take a long time to complete depending on the directory size of your server.
- **Customized scan** – This can be configured to scan the following file paths where malicious files from the threat actor have been observed:
- *%IIS installation path%\aspnet_client\**
- *%IIS installation path%\aspnet_client\system_web\**
- *%Exchange Server installation path%\FrontEnd\HttpProxy\owa\auth\**
- *Configured temporary ASP.NET files path*
- *%Exchange Server Installation%\FrontEnd\HttpProxy\ecp\auth\**

These remediation steps are effective against known attack patterns but are **not guaranteed as complete mitigation for all possible exploitation** of these vulnerabilities. Microsoft Defender will continue to monitor and provide the latest security updates.