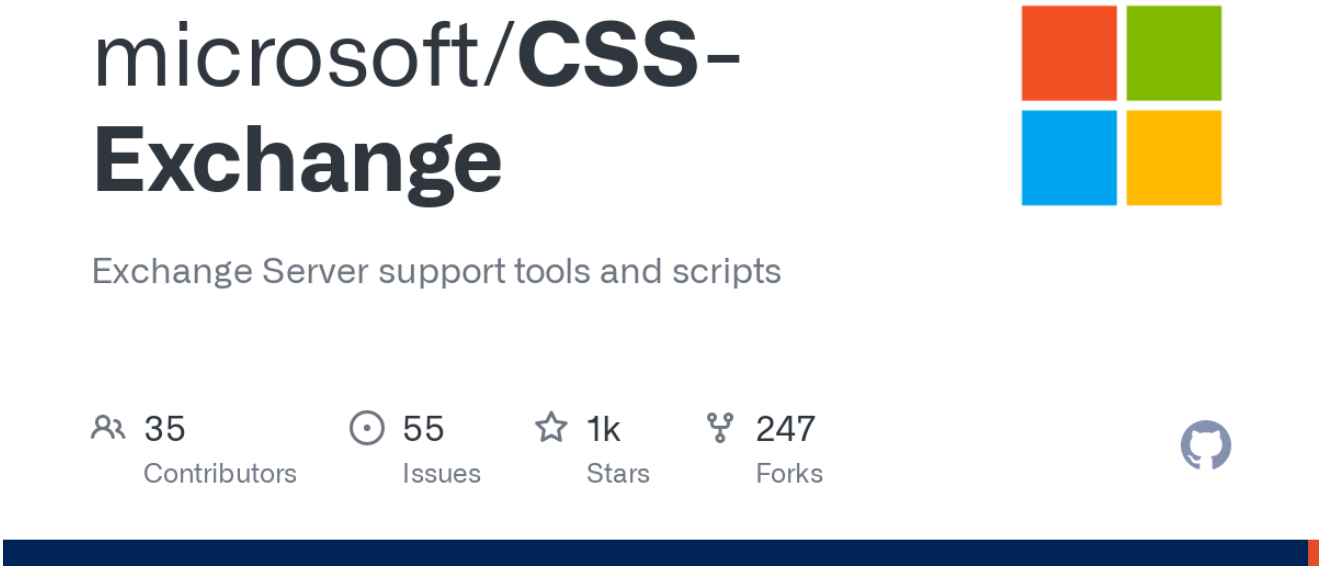
Security scripts

github.com/microsoft/CSS-Exchange/tree/main/Security

microsoft



Apply new code keyword casing rule

`43004e6`

Failed to load latest commit information.

Script	More Info	Download
EOMT	More Info	Download
ExchangeMitigations.ps1	More Info	Obsolete
http-vuln-cve2021-26855.nse	More Info	Obsolete
Test-ProxyLogon.ps1	More Info	Download

Exchange On-premises Mitigation Tool (EOMT)

This script contains mitigations to help address the following vulnerabilities.

CVE-2021-26855

This is the most effective way to help quickly protect and mitigate your Exchange Servers prior to patching. **We recommend this script over the previous ExchangeMitigations.ps1 script.** The Exchange On-premises Mitigation Tool automatically downloads any dependencies and runs the Microsoft Safety Scanner. This a better approach for Exchange deployments with Internet access and for those who want an attempt at automated remediation. We have not observed any impact to Exchange Server functionality via these mitigation methods. EOMT.ps1 is completely automated and uses familiar mitigation methods previously documented. This script has four operations it performs:

- ***+NEW*** Check for the latest version of EOMT and download it.
- Mitigate against current known attacks using CVE-2021-26855 via a URL Rewrite configuration
- Scan the Exchange Server using the Microsoft Safety Scanner
- Attempt to remediate compromises detected by the Microsoft Safety Scanner.

This a better approach for Exchange deployments with Internet access and for those who want an attempt at automated remediation. We have not observed any impact to Exchange Server functionality via these mitigation methods nor do these mitigation methods make any direct changes that disable features of Exchange.

Use of the Exchange On-premises Mitigation Tool and the Microsoft Saftey Scanner are subject to the terms of the Microsoft Privacy Statement: https://aka.ms/privacy

Requirements to run the Exchange On-premises Mitigation Tool

- External Internet Connection from your Exchange server (required to download the Microsoft Safety Scanner and the IIS URL Rewrite Module).
- PowerShell script must be run as Administrator.

System Requirements

- PowerShell 3 or later
- IIS 7.5 and later
- Exchange 2013, 2016, or 2019
- Windows Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Server 2019

- ***+New*** If Operating System is older than Windows Server 2016, must have KB2999226 for IIS Rewrite Module 2.1 to work.

Who should run the Exchange On-premises Mitigation Tool

Situation	Guidance
If you have done nothing to date to patch or mitigate this issue…	Run EOMT.PS1 as soon as possible.This will both attempt to remediate as well as mitigate your servers against further attacks. Once complete, follow patching guidance to update your servers on http://aka.ms/exchangevulns
If you have mitigated using any/all of the mitigation guidance Microsoft has given (Exchangemitigations.Ps1, Blog post, etc..)	Run EOMT.PS1 as soon as possible. This will both attempt to remediate as well as mitigate your servers against further attacks. Once complete, follow patching guidance to update your servers on http://aka.ms/exchangevulns
If you have already patched your systems and are protected, but did NOT investigate for any adversary activity, indicators of compromise, etc….	Run EOMT.PS1 as soon as possible. This will attempt to remediate any existing compromise that may not have been full remediated before patching.
If you have already patched and investigated your systems for any indicators of compromise, etc….	No action is required

Important note regarding Microsoft Safety Scanner

The Exchange On-premises Mitigation Tool runs the Microsoft Safety Scanner in a quick scan mode. If you suspect any compromise, we highly recommend you run it in the FULL SCAN mode. FULL SCAN mode can take a long time but if you are not running Microsoft Defender AV as your default AV, FULL SCAN will be required to remediate threats.

Exchange On-premises Mitigation Tool Examples

The default recommended way of using EOMT.ps1. This will determine if your server is vulnerable, mitigate if vulnerable, and run MSERT in quick scan mode. If the server is not vulnerable only MSERT quick scan will run.

```
.\EOMT.ps1
```

To run a Full MSERT Scan - We only recommend this option only if the initial quick scan discovered threats. The full scan may take hours or days to complete.

```
.\EOMT.ps1 -RunFullScan -DoNotRunMitigation
```

To run the Exchange On-premises Mitigation Tool with MSERT in detect only mode - MSERT will not remediate detected threats.

```
.\EOMT.ps1 -DoNotRemediate
```

To roll back the Exchange On-premises Mitigation Tool mitigations

```
.\EOMT.ps1 -Rollbackmitigation
```

Note: If ExchangeMitigations.ps1 was used previously to apply mitigations, Use ExchangeMitigations.ps1 for rollback.

+NEW EOMT will now autoupdate by downloading the latest version from GitHub. To prevent EOMT from fetching updates to EOMT.ps1 from the internet.

```
.\EOMT.ps1 -DoNotAutoUpdateEOMT
```

Exchange On-premises Mitigation Tool Q & A

Question: What mode should I run EOMT.ps1 in by default?

Answer: By default, EOMT.ps1 should be run without any parameters:

This will run the default mode which does the following:

1. Checks if your server is vulnerable based on the presence of the SU patch or Exchange version.
2. Downloads and installs the IIS URL rewrite tool **(only if vulnerable)**.
3. Applies the URL rewrite mitigation **(only if vulnerable)**.
4. Runs the Microsoft Safety Scanner in "Quick Scan" mode **(vulnerable or not)**.

Question: What if I run a full scan and it’s affecting the resources of my servers?

Answer: You can terminate the process of the scan by running the following command in an Administrative PowerShell session.

```
Stop-Process -Name msert
```

Question: What is the real difference between this script (EOMT.PS1) and the previous script Microsoft released (ExchangeMitigations.Ps1).

Answer: The Exchange On-premises Mitigation Tool was released to help pull together multiple mitigation and response steps, whereas the previous script simply enabled mitigations. Some details on what each do:

EOMT.PS1

- Mitigation of CVE-2021-26855 via a URL Rewrite configuration.
- Mitigation does not impact Exchange functionality.
- Malware scan of the Exchange Server via the Microsoft Safety Scanner
- Attempt to reverse any changes made by identified threats.

ExchangeMitigations.ps1:

- Does mitigations for all 4 CVE's - CVE-2021-26855, CVE-2021-26857, CVE-2021-27065 & CVE-2021-26858.
- Some of the mitigation methods impact Exchange functionality.
- Does not do any scanning for existing compromise or exploitation.
- Does not take response actions to existing active identified threats.

Question: What if I do not have an external internet connection from my Exchange server?

Answer: If you do not have an external internet connection, you can still use the legacy script (ExchangeMitigations.ps1) and other steps from the mitigation blog post: Microsoft Exchange Server Vulnerabilities Mitigations – March 2021

Question: If I have already ran the mitigations previously, will the Exchange On-premises Mitigation Tool roll back any of the mitigations?

Answer: No, please use the legacy script (ExchangeMitigations.ps1) to do rollback. The legacy script supports rollback for the mitigations the Exchange On-premises Mitigation Tool applied.

Test-ProxyLogon.ps1

Formerly known as Test-Hafnium, this script automates all four of the commands found in the Hafnium blog post. It also has a progress bar and some performance tweaks to make the CVE-2021-26855 test run much faster.

Download the latest release here:

Download Test-ProxyLogon.ps1

Usage

The most typical usage of this script is to check all Exchange servers and save the reports, by using the following syntax from Exchange Management Shell:

```
Get-ExchangeServer | .\Test-ProxyLogon.ps1 -OutPath $home\desktop\logs
```

To check the local server only, just run the script:

```
.\Test-ProxyLogon.ps1 -OutPath $home\desktop\logs
```

To check the local server and copy the identified logs and files to the OutPath:

```
.\Test-ProxyLogon.ps1 -OutPath $home\desktop\logs -CollectFiles
```

To display the results without saving them, pass -DisplayOnly:

```
.\Test-ProxyLogon.ps1 -DisplayOnly
```

Frequently Asked Questions

The script says it found suspicious files, and it lists a bunch of zip files. What does this mean?

The script will flag any zip/7x/rar files that it finds in ProgramData. As noted in this blog post, web shells have been observed using such files for exfiltration. An administrator should review the files to determine if they are valid. Determining if a zip file is a valid part of an installed product is outside the scope of this script, and whitelisting files by name would only encourage the use of those specific names by attackers.

I'm having trouble running the script on Exchange 2010.

If PowerShell 3 is present, the script can be run on Exchange 2010. It will not run-on PowerShell 2. One can also enable PS Remoting and run the script remotely against Exchange 2010. However, the script has minimal functionality in these scenarios, as Exchange 2010 is only affected by one of the four announced exploits - CVE-2021-26857. Further, this exploit is only available if the Unified Messaging role is present. As a result, it is often easier to simply run the Get-EventLog command from the blog post, rather than using Test-ProxyLogon.

ExchangeMitigations.ps1

NOTE: This script is obsolete and is no longer maintained. Please use EOMT.ps1 instead.

The final release can be downloaded here:

Download ExchangeMitigations.ps1

This script contains 4 mitigations to help address the following vulnerabilities:

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

For more information on each mitigation please visit https://aka.ms/exchangevulns

This should only be used as a temporary mitigation until your Exchange Servers can be fully patched, recommended guidance is to apply all of the mitigations at once.

For this script to work you must have the IIS URL Rewrite Module installed which can be done via this script using the -FullPathToMSI parameter.

URL Rewrite Module 2.1 must be installed, you can download version 2.1 here:

x86 & x64 -https://www.iis.net/downloads/microsoft/url-rewrite

For systems running IIS 8.5 and lower KB2999226 must be installed. Please review the pre-reqs for this KB and download from https://support.microsoft.com/en-us/topic/update-for-universal-c-runtime-in-windows-c0514201-7fe6-95a3-b0a5-287930f3560c"

Script requires PowerShell 3.0 and later and must be executed from an elevated PowerShell Session.

To apply all mitigations with MSI install

```
.\ExchangeMitigations.ps1 -FullPathToMSI "FullPathToMSI" -WebSiteNames "Default Web Site" -ApplyAllMitigations
```

To apply all mitigations without MSI install

```
.\ExchangeMitigations.ps1 -WebSiteNames "Default Web Site" -ApplyAllMitigations -Verbose
```

To rollback all mitigations

```
.\ExchangeMitigations.ps1 -WebSiteNames "Default Web Site" -RollbackAllMitigation
```

To apply multiple or specific mitigations (out of the 4)

```
.\ExchangeMitigations.ps1 -WebSiteNames "Default Web Site" -ApplyECPAppPoolMitigation -ApplyOABAppPoolMitigation
```

To rollback multiple or specific mitigations

```
.\ExchangeMitigations.ps1 -WebSiteNames "Default Web Site" -RollbackECPAppPoolMitigation -RollbackOABAppPoolMitigation
```

http-vuln-cve2021-26855.nse

NOTE: This file is obsolete and is no longer maintained. Please use EOMT.ps1 instead.

The final release can be downloaded here:

Download http-vuln-cve2021-26855.nse

This file is for use with nmap. It detects whether the specified URL is vulnerable to the Exchange Server SSRF Vulnerability (CVE-2021-26855). For usage information, please read the top of the file.