# Tài liệu hướng dẫn vá lỗ hổng bảo mật trong Microsoft Exchange Server

Tháng 03, 2021

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC)

Cục An toàn thông tin

# MỤC LỤC

# Chương 1: Thông tin về lỗ hổng Microsoft Exchange Server

## 1.1. Tổng quan

Email là công cụ trao đổi thông tin phổ biến được hầu hết các cơ quan tổ chức sử dụng. Hiện nay, Microsoft Exchange Server là ứng dụng thư điện tử sử dụng nhiều trong cơ quan tổ chức để quản lý hệ thống thư điện tử. Ứng dụng Mail Exchange của Microsoft là một trong những công cụ được đánh giá cao bởi tính ổn định, an toàn và bảo mật cao mà dịch vụ mail này mang lại. Do vậy, công cụ này là mục tiêu hàng đầu mà đối tượng tấn công nhắm đến để đánh cắp thông tin nhạy cảm.

Ngày 02/03/2021, Microsoft đã công bố bản vá cho các lỗ hổng bảo mật **(CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)** ảnh hưởng **nghiêm trọng** đến máy chủ Microsoft Exchange. Các lỗ hổng này ảnh hưởng tới các phiên bản Microsoft Exchange Server 2013/2016/2019, cho phép đối tượng tấn công truy cập vào máy chủ hệ thống, thực thi mã từ xa.

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đã có văn bản số 11 /NCSC –ĐTPT vào ngày 03/03/2021 cảnh báo rộng rãi về lỗ hổng bảo mật này.

## 1.2. Thông tin các lỗ hổng bảo mật

| TT | CVE | Mô tả | Link tham khảo hướng dẫn |
|---|---|---|---|
| 1 | CVE-2021-26855 | Điểm CVSS: 9.1 (cao)<br>Cho phép đối tượng tấn công thực hiện tấn công SSRF | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26855 |
| 2 | CVE-2021-26857 | Điểm CVSS: 7.8 (cao)<br>Lỗi insecure deserialization, cho phép đối tượng tấn công thực thi mã với quyền hệ thống. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857 |
| 3 | CVE-2021-26858 | Điểm CVSS: 7.8 (cao)<br>Cho phép đối tượng tấn công ghi file tùy ý sau xác thực. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858 |
| 4 | CVE-2021-27065 | Điểm CVSS: 7.8 (cao)<br>Cho phép đối tượng tấn công ghi file tùy ý sau xác thực. | https://msrc.microsoft.com/update- |

| | | | |
|---|---|---|---|
| | | | guide/vulnerability/CVE-2021-27065 |

### 1.3. Thông tin các phiên bản ảnh hưởng và bản vá

| TT | Phiên bản ảnh hưởng | Bản cập nhật |
|---|---|---|
| 1 | Exchange Server 2013 | https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-march-2-2021-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b |
| 2 | Exchange Server 2016 | https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-march-2-2021-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b |
| 3 | Exchange Server 2019 | https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-march-2-2021-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b |

## Chương 2: Hướng dẫn khắc phục

Quy trình các bước thực hiện khắc phục như sau:

- Bước 1: Xác định hệ thống có tồn tại lỗ hổng hay không

- Bước 2: Kiểm tra tìm kiếm các dấu hiếu bị khai thác

- Bước 3: Nếu tồn tại lỗ hổng, cập nhật bản vá

- Bước 4: Trong trường hợp chưa thể cập nhật ngay, thực hiện các biện pháp khắc phục thay thế

## 2.1. Hướng dẫn xác định lỗ hổng có trên hệ thống hay không

Quý đơn vị có thể kiểm tra hệ thống máy chủ thư điện tử có tồn tại lỗ hổng hay không bằng công cụ Trung tâm NCSC đã xây dựng tại địa chỉ: https://khonggianmang.vn/check-proxylogon


Nhập vào tên miền địa chỉ mail sau đó nhấn **KIỂM TRA**, nếu hệ thống có lỗi sẽ nhận được thông báo:


## 2.2. Hướng dẫn các bước phát hiện dấu hiệu khai thác

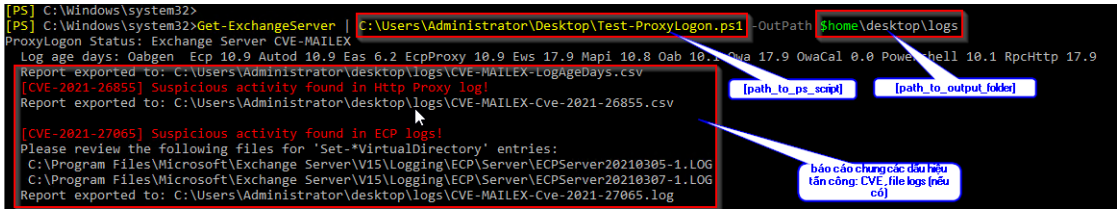
Để giúp điều tra phát hiện dấu hiệu tấn công, Microsoft đã phát hành một tập lệnh PowerShell có tên là Test-ProxyLogon.ps1 tại địa chỉ:

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

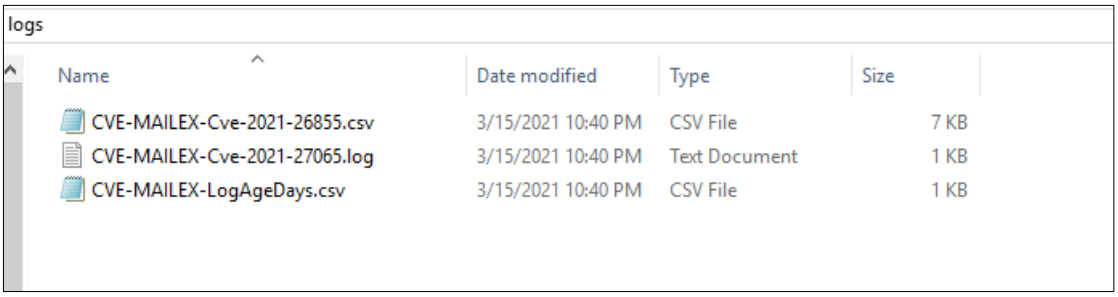
Quý đơn vị tải xuống và thực hiện theo hướng dẫn sau:

- Mở "**Exchange Management Shell**"
- Kiểm tra tất cả các máy chủ Exchange của Quý đơn vị và lưu logs vào máy tính sử dụng lệnh:

```
Get-ExchangeServer | [path_to_ps_script] -OutPath [path_to_output_folder]
```

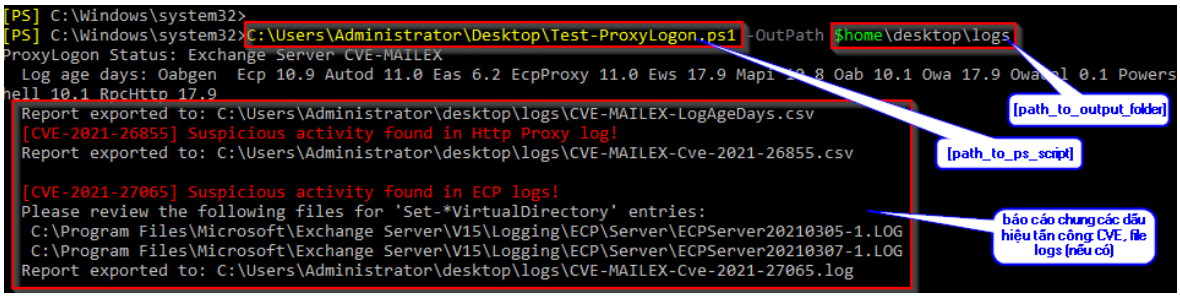



Vào thư mục được lưu logs để xem chi tiết:

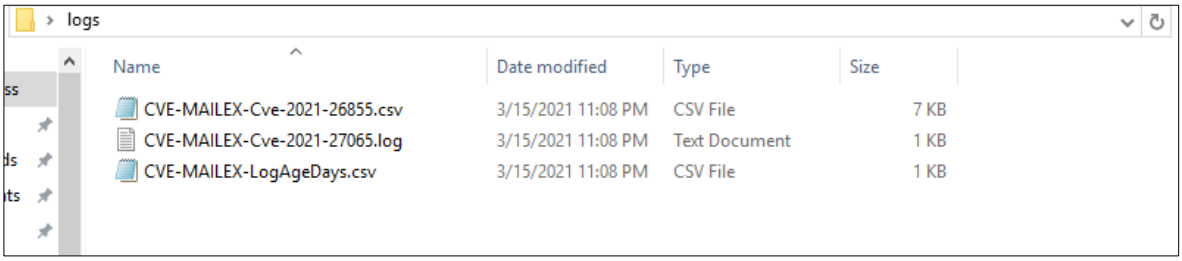



- Nếu chỉ muốn kiểm tra máy chủ cục bộ và lưu logs, sử dụng lệnh:

| |
|---|
| [path_to_ps_script] -OutPath [path_to_output_folder] |

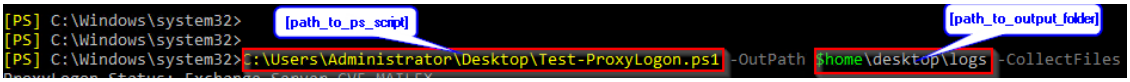



Vào thư mục được lưu logs để xem chi tiết kết quả:

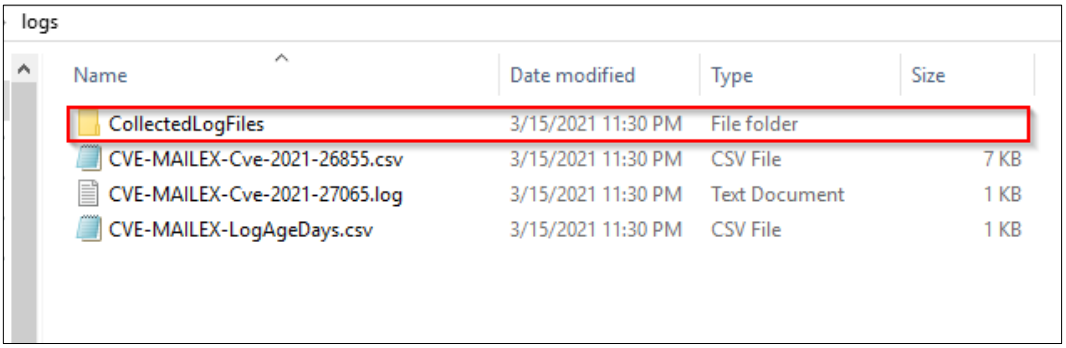



- Để kiểm tra máy chủ cục bộ, sao chép các tệp tin và log đã xác định, truy cập vào OutPath:

| |
|---|
| [path_to_ps_script] -OutPath [path_to_output_folder] |



Vào thư mục được lưu logs để xem chi tiết kết quả:




- Để kiểm tra máy chủ cục bộ và hiển thị kết quả mà không lưu, sử dụng lệnh:

| |
|---|
| [path_to_ps_script] -DisplayOnly |

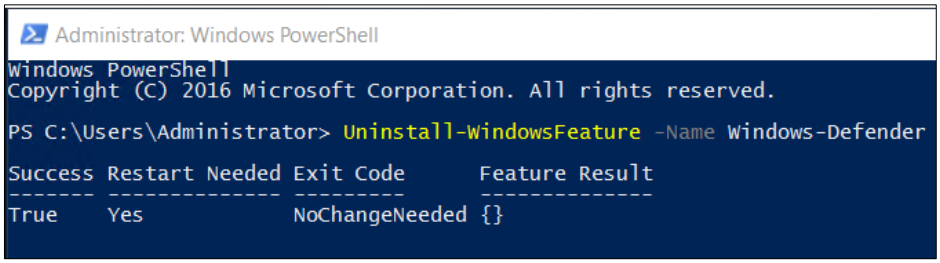

Trong trường hợp này, các file log chi tiết sẽ không được lưu lại

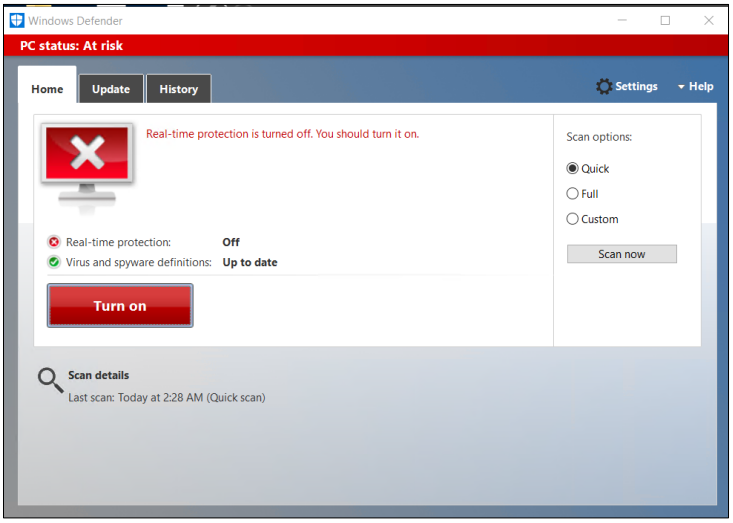
## 2.3. Hướng dẫn cập nhật bản vá

Microsoft đã phát hành bản vá cho lỗ hổng ProxyLogon, các quản trị viên nên cập nhật ngay khi có thể. Các bước thực hiện theo khuyến nghị của Microsoft (https://techcommunity.microsoft.com/t5/exchange-team-blog/march-2021-exchange-server-security-updates-for-older-cumulative/ba-p/2192020) như sau:

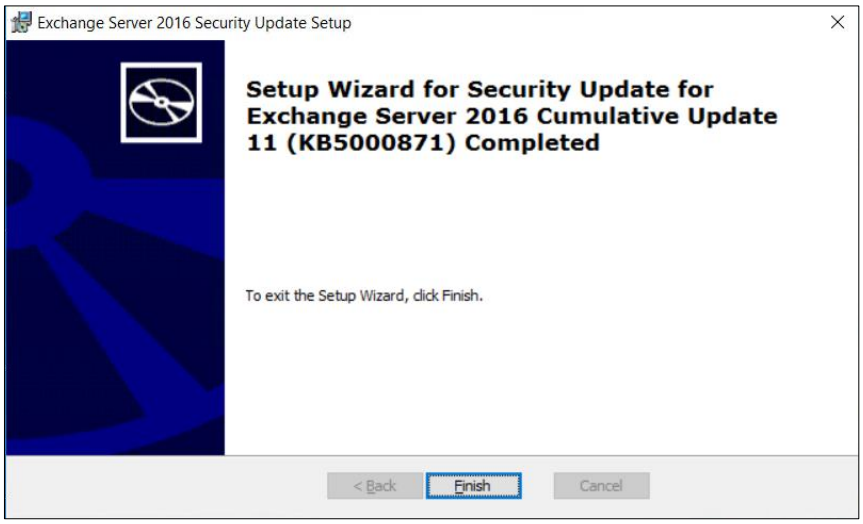
- Kiểm tra phiên bản Exchange hiện tại: Vào chức năng Start > Microsoft Exchange Server > Exchange Management Shell rồi gõ lệnh **Get-ExchangeServer | Format-List AdminDisplayVersion** để xem phiên bản Exchange hiện tại trên hệ thống
- Tải về bản cập nhật ứng với phiên bản hiện tại của hệ thống tại: https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-march-2-2021-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b

- Vô hiệu hóa phần mềm antivirus: Mở PowerShell và nhập lệnh **Uninstall-WindowsFeature -Name Windows-Defender** rồi nhấn **Enter**. Sau khi thực hiện xong lệnh > **Restart** lại máy tính




- Chạy file cài đặt (file .msp) đã tải về bằng Command Prompt với quyền quản trị:
    - Nhập **cmd** trong hộp tìm kiếm trong Windows > kích chuột phải **vào Command Prompt** > **Run as administrator > Yes >** nhập đường dẫn tuyệt đối của **file .msp** đã tải về vào giao diện Command Prompt rồi nhấn Enter để cài đặt bản cập nhật.
    - Chờ cho đến khi quá trình chuẩn bị cài đặt hoàn tất rồi nhấn **Next** > **I accept the License Terms** > **Next** > Chờ đến khi quá trình cập nhật hoàn tất > **Finish**.
- Kích hoạt lại phần mềm antivrus bằng lệnh **Install-WindowsFeature -Name Windows-Defender** rồi nhấn **Enter** và khởi động lại hệ thống để hoàn tất quá trình cập nhật.




- Kiểm tra lại hệ thống đã được vá lỗi sau khi cập nhật bản vá chưa theo hướng dẫn trong mục 2.1.

### 2.4. Hướng dẫn các bước khắc phục giảm thiểu

Trong trường hợp chưa thể cập nhật bản vá ngay, Quý đơn vị có thể sử dụng biện pháp thay thế tạm thời nhằm giảm thiểu tác động. Tuy nhiên các biện pháp này không phải là biện pháp khắc phục trong trường hợp các máy chủ Exchange đã bị tấn công và cũng không đảm bảo sẽ bảo vệ hệ thống một cách toàn diện khỏi cuộc tấn công. Trung tâm NCSC khuyến nghị đơn vị thực hiện các bước điều tra song song hoặc sau khi áp dụng các biện pháp giảm thiểu thay thế.

Công cụ sử dụng: "one-click mitigation tool" (Exchange On-premises Mitigation Tool) của Microsoft có tại: https://github.com/microsoft/CSS-Exchange/releases/latest/download/EOMT.ps1

**Ghi chú:** - Tập lệnh này dùng để xử lý giảm thiểu rủi ro đối với CVE-2021-26855 – điểm bắt đầu của chuỗi 4 lỗ hổng

- Việc sử dụng công cụ này chưa phát hiện ra các ảnh hưởng đến chức năng của máy chủ Exchange.

Để chạy công cụ Exchange On-premises Mitigation Tool (EOMT), cần:

- Có thể kết nối Internet ra bên ngoài từ máy chủ Exchange (để tải xuống Microsoft Safety Scanner và IIS URL Rewrite Module).
- Tập lệnh PowerShell (EOMT.ps1) phải chạy dưới quyền Administrator.

Các yêu cầu về hệ thống:

- PowerShell từ phiên bản 3 trở lên
- IIS từ phiên bản 7.5 trở lên

- Exchange 2013, 2016, 2019
- Windows Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Server 2019

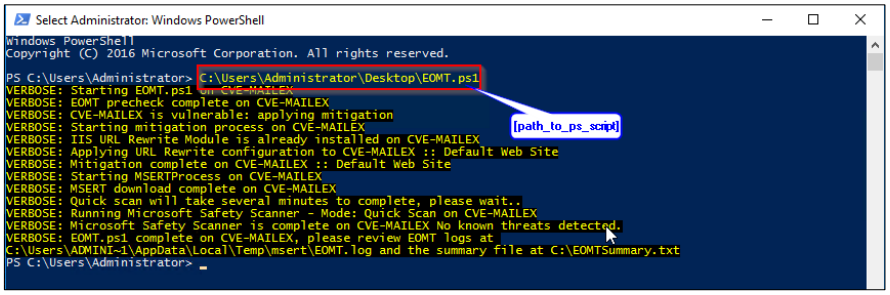
Hướng dẫn sử dụng công cụ EOMT:

- Để chạy tool ở chế độ mặc định, chạy câu lệnh sau:

```
[path_to_ps_script]
```

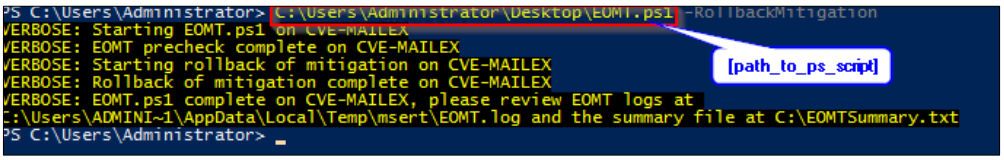
Chế độ mặc định sẽ thực hiện các việc sau:

- ➢ Kiểm tra xem máy chủ của bạn có dễ bị tấn công hay không dựa trên bản vá cập nhật hoặc phiên bản Exchange
- ➢ Tải xuống và cài đặt công cụ IIS URL rewrite.
- ➢ Áp dụng URL Rewrite Mitigation (chỉ khi có lỗ hổng).
- ➢ Chạy Microsoft Safety Scanner ở chế độ "Quét nhanh".



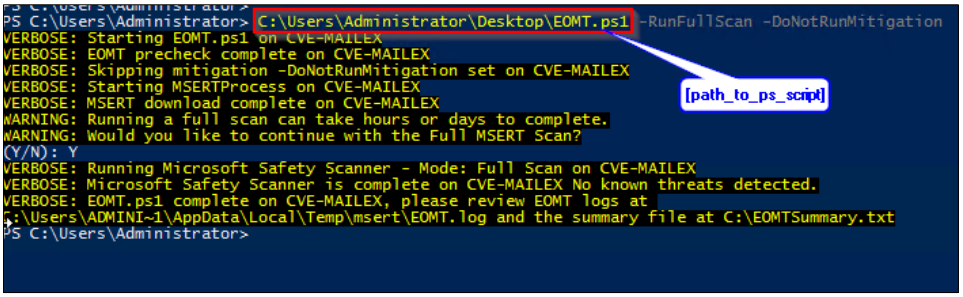

- Để khôi phục URL Rewrite Mitigation, chạy câu lệnh sau:

```
[path_to_ps_script] -RollbackMitigation
```




- Nếu chỉ muốn Chạy Microsoft Safety Scanner ở chế độ "Quét toàn bộ", chạy câu lệnh sau:

```
[path_to_ps_script] -RunFullScan -DoNotRunMitigation
```



***Ghi chú:*** *Nên chạy câu lệnh này khi quá trình quét nhanh ban đầu phát hiện ra các dấu hiệu của cuộc tấn công. Quá trình quét toàn bộ có thể mất vài giờ hoặc vài ngày để hoàn thành.*

Ngoài ra Quý đơn vị có thể tham khảo các biện pháp giảm thiểu (tại phụ lục kèm theo).

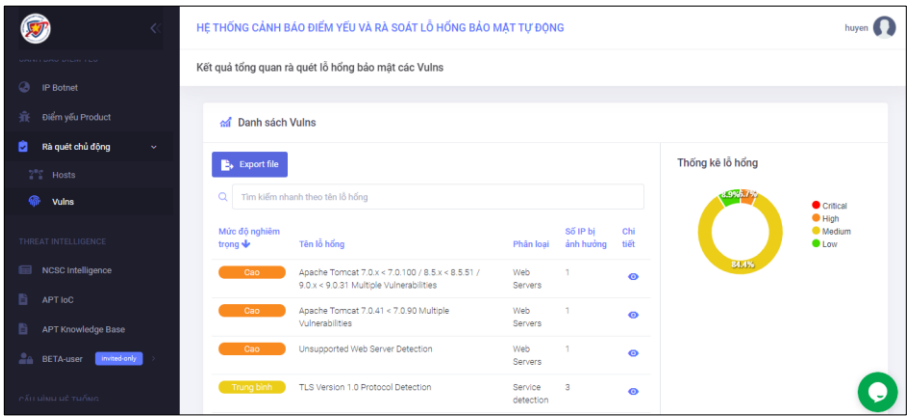
**Tổng kết:**

Trên đây là các bước thực hiện khắc phục lỗ hổng. Trong trường hợp phát hiện đã bị tấn công, Quý đơn vị cần rà soát và xử lý ngay.

Ngoài kiểm tra và cập nhật bản vá, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) khuyến nghị Quý đơn vị nên cài đặt thêm công cụ rà quét, loại bỏ mã độc để kiểm tra thêm.

Tham khảo công cụ của Microsoft tại địa chỉ: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download

Bên cạnh đó, "HỆ THỐNG CẢNH BÁO ĐIỂM YẾU VÀ RÀ SOÁT LỖ HỔNG BẢO MẬT TỰ ĐỘNG" của Trung tâm NCSC tại địa chỉ: https://service.khonggianmang.vn/ cũng hỗ trợ Quý đơn vị giám sát, theo dõi hệ thống của mình để có các cảnh báo sớm, từ đó đưa ra các phương án xử lý kịp thời với các chức năng như: rà quét chủ động (cảnh báo các địa chỉ IP bị ảnh hưởng, các lỗ hổng tồn tại), tin tức cảnh báo kỹ thuật,…



## Phụ lục

### Hướng dẫn các bước giảm thiểu khắc phục khác (không sử dụng công cụ)

Các biện pháp giảm thiểu bao gồm:

- Triển khai một IIS Re-Write Rule để lọc các yêu cầu https độc hại
- Vô hiệu hóa Unified Messaging (UM)
- Vô hiệu hóa Exchange Control Panel (ECP) VDir
- Vô hiệu hóa Offline Address Book (OAB) Vdir

Các biện pháp này hiệu quả trong việc giảm thiểu nguy cơ tấn công đã biết trong thời gian gần đây, nhưng không đảm bảo là có thể thay thế và phòng chống hoàn toàn vào các khai thác có thể xảy ra đối với lỗ hổng này. Đây là biện pháp tạm thời cho đến khi có thể vá hoàn toàn các máy chủ Exchange, Trung tâm NCSC khuyến nghị nên áp dụng tất cả biện pháp nêu trên.

**Ghi chú:** Các biện pháp này có thể được áp dụng hoặc khôi phục lại bằng cách sử dụng tập lệnh ExchangeMitigations.ps1và có một số tác động đối với chức năng của máy chủ Exchange.

**1. Backend Cookie Mitigation (áp dụng cho CVE-2021-26855)**

**- Mô tả:** Biện pháp này sẽ lọc các yêu cầu https có chứa X-AnonResource-Backend độc hại và cookie X-BEResource không đúng định dạng (được phát hiện sử dụng trong các cuộc tấn công SSRF trên Internet). Điều này sẽ giúp chống lại các mô hình đã biết nhưng không phải là toàn bộ SSRF.

**- Yêu cầu:** Mô-đun URL Rewrite

Đối với IIS phiên bản 10 trở lên nên sử dụng URL Rewrite Module 2.1 (x86 và x64), tải xuống tại:

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

Đối với IIS phiên bản 8.5 trở xuống nên sử dụng URL Rewrite Module 2.0, tải xuống tại:

**x86**: https://www.microsoft.com/en-us/download/details.aspx?id=5747
**x64**: https://www.microsoft.com/en-us/download/details.aspx?id=7435

**- Ảnh hưởng:** Chưa phát hiện các ảnh hưởng đối với chức năng của máy chủ Exchange nếu mô-đun URL Rewrite được cài đặt.

Các IIS Rewrite rule sẽ bị xóa sau khi Exchange được nâng cấp và biện pháp này sẽ cần được áp dụng lại nếu bản vá bảo mật chưa được cài đặt.

**2. Unified Messaging Mitigation (áp dụng cho CVE-2021-26857)**

**- Mô tả:** Biện pháp này sẽ vô hiệu hóa dịch vụ Unified Messaging và dịch vụ Exchange Managed Availability trong Exchange.

**- Ảnh hưởng:** Unified Messaging/Voicemail ngừng hoạt động khi các dịch vụ này bị vô hiệu hóa. Khả năng giám sát nâng cao của Exchange cũng bị vô hiệu hóa, do vô hiệu hóa dịch vụ Microsoft Exchange Managed Availability.

**3. ECP Application Pool Mitigation (áp dụng cho CVE-2021-27065, CVE-2021-26858)**

**- Mô tả:** Biện pháp này sẽ vô hiệu hóa dịch vụ Exchange Control Panel (ECP) Virtual Directory và Microsoft Exchange Managed Availability

**- Ảnh hưởng:** Exchange Control Panel sẽ không còn khả dụng. Khả năng giám sát nâng cao của Exchange cũng bị vô hiệu hóa do dịch vụ Microsoft Exchange Managed Availability bị vô hiệu hóa.

**4. OAB Application Pool Mitigation (áp dụng cho CVE-2021-27065, CVE-2021-26858)**

**- Mô tả:** Biện pháp này vô hiệu hóa nhóm ứng dụng Offline Address Book (OAB) và API. Dịch vụ Microsoft Exchange Managed Availability cũng bị vô hiệu hóa.

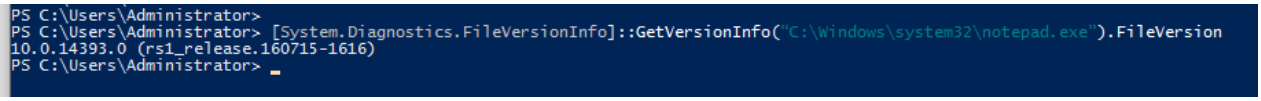
**- Ảnh hưởng:** OAB sẽ không khả dụng, bao gồm cả việc tải xuống của OAB bởi Outlook clients. Khả năng giám sát nâng cao của Exchange cũng bị vô hiệu hóa, do vô hiệu hóa dịch vụ Microsoft Exchange Managed Availability.

**Sử dụng tập lệnh ExchangeMitigations.ps1 để triển khai các biện pháp trên**

- Để tập lệnh này hoạt động, máy chủ cần phải cài đặt IIS URL Rewrite Module, điều này có thể thực hiện khi chạy tập lệnh **ExchangeMitigations.ps1** với tham số **-FullPathToMSI**.

**Bước 1:** Kiểm tra phiên bản của IIS bằng cách mở Window PowerShell và chạy lệnh sau:

```
[System.Diagnostics.FileVersionInfo]::GetVersionInfo("C:\Windows\system32\notepad.exe").FileVersion
```

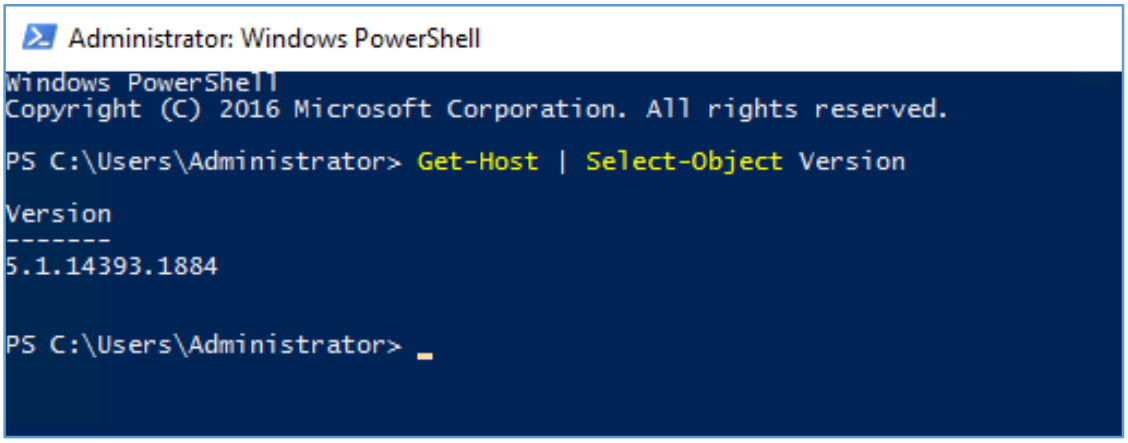


**Bước 2:** Tải xuống file cài đặt (.msi file) thích hợp cho IIS URL Rewrite Module theo hướng dẫn ở **mục 2.4.1.**

Có thể cài đặt IIS URL Rewrite Module bằng file .msi vừa tải xuống hoặc sử dụng tham số -FullPathToMSI trong quá trình chạy tập lệnh.

- Ngoài ra, tập lệnh này yêu cầu chạy trên PowerShell phiên bản 3.0 hoặc cao hơn và phải được thực thi bởi PowerShell bằng quyền cao hơn. Phiên bản của PowerShell có thể được kiểm tra bằng cách mở PowerShell và chạy câu lệnh sau:

```
Get-Host | Select-Object Version
```




Tải xuống phiên bản mới nhất tại: https://github.com/microsoft/CSS-Exchange/releases/latest/download/ExchangeMitigations.ps1

**Bước 3:** Mở Window PowerShell bằng quyền cao hơn và thêm exchange Cmdlets snap-in vào PowerShell hiện tại bằng câu lệnh:

- Exchange 2007

```
Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin
```

- Exchange 2010

```
Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010
```

- Exchange 2013 & 2016

```
Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn
```

**Để áp dụng:**

- Tất cả biện pháp không cài đặt MSI (trong trường hợp đã cài đặt IIS URL Rewrite Module), chạy câu lệnh sau:

```
[path_to_ps_script] -WebSiteNames "Default Web Site" -
ApplyAllMitigations
```

```
PS C:\Users\Administrator> C:\Users\Administrator\Desktop\ExchangeMitigations.ps1 -WebSiteNames 'Default Web Site' -ApplyAllMitigations
VERBOSE: [INFO] IIS URL Rewrite Module 2 already installed on CVE-MAILEX

name                   : X-AnonResource-Backend Abort - inbound
enabled                : True
patternSyntax          : ECMAScript
stopProcessing         : False
responseCacheDirective : Auto
match                  : Microsoft.IIs.PowerShell.Framework.ConfigurationElement
conditions             : Microsoft.IIs.PowerShell.Framework.ConfigurationElement
serverVariables        : Microsoft.IIs.PowerShell.Framework.ConfigurationElement
action                 : Microsoft.IIs.PowerShell.Framework.ConfigurationElement
PSPath                 : MACHINE/WEBROOT/APPHOST/Default Web Site
Location               :
ConfigurationPathType  : Location
ItemXPath              : /system.webServer/rewrite/rules/rule[@name='X-AnonResource-Backend Abort - inbound']
Attributes             : {name, enabled, patternSyntax, stopProcessing...}
ChildElements          : {match, conditions, serverVariables, action}
ElementTagName         : rule
Methods                :
Schema                 : Microsoft.IIs.PowerShell.Framework.ConfigurationElementSchema

name                   : X-BEResource Abort - inbound
enabled                : True
patternSyntax          : ECMAScript
stopProcessing         : True
responseCacheDirective : Auto
match                  : Microsoft.IIs.PowerShell.Framework.ConfigurationElement
conditions             : Microsoft.IIs.PowerShell.Framework.ConfigurationElement
serverVariables        : Microsoft.IIs.PowerShell.Framework.ConfigurationElement
action                 : Microsoft.IIs.PowerShell.Framework.ConfigurationElement
PSPath                 : MACHINE/WEBROOT/APPHOST/Default Web Site
Location               :
ConfigurationPathType  : Location
ItemXPath              : /system.webServer/rewrite/rules/rule[@name='X-BEResource Abort - inbound']
Attributes             : {name, enabled, patternSyntax, stopProcessing...}
ChildElements          : {match, conditions, serverVariables, action}
ElementTagName         : rule
Methods                :
Schema                 : Microsoft.IIs.PowerShell.Framework.ConfigurationElementSchema
```

[path_to_ps_script]

```
Status      : Stopped
Name        : MSExchangeHM
DisplayName : Microsoft Exchange Health Manager

Status      : Stopped
Name        : MSExchangeHMRecovery
DisplayName : Microsoft Exchange Health Manager Recovery

Status      : Stopped
Name        : MSExchangeUM
DisplayName : Microsoft Exchange Unified Messaging

Status      : Stopped
Name        : MSExchangeUMCR
DisplayName : Microsoft Exchange Unified Messaging Call Router

Status      : Stopped
Name        : MSExchangeHM
DisplayName : Microsoft Exchange Health Manager

Status      : Stopped
Name        : MSExchangeHMRecovery
DisplayName : Microsoft Exchange Health Manager Recovery

VERBOSE: Performing the operation "Set-Item" on target "-path \\CVE-MAILEX\AppPools\MSExchangeECPAppPool".
VERBOSE: Status of MSExchangeECPAppPool
Value : Stopped

Status      : Stopped
Name        : MSExchangeHM
DisplayName : Microsoft Exchange Health Manager

Status      : Stopped
Name        : MSExchangeHMRecovery
DisplayName : Microsoft Exchange Health Manager Recovery

VERBOSE: Performing the operation "Set-Item" on target "-path \\CVE-MAILEX\AppPools\MSExchangeOABAppPool".
VERBOSE: Status of MSExchangeOABAppPool
Value : Stopped
```

- Để áp dụng tất cả biện pháp, đồng thời cài đặt MSI, chạy câu lệnh sau:

| |
|---|
| [path_to_ps_script] -FullPathToMSI [fullpath_to_msi_file] -WebSiteNames ‘Default Web Site’ -ApplyAllMitigations |

(Kết quả tương tự như trường hợp trên)

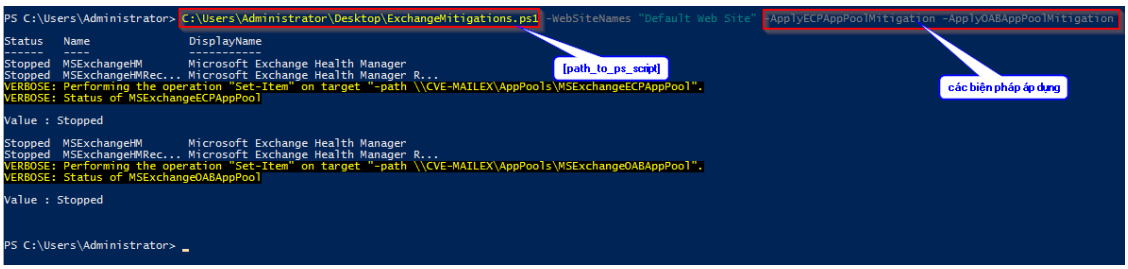
- Để áp dụng nhiều hoặc một biện pháp cụ thể, chạy câu lệnh sau:

| |
|---|
| [path_to_ps_script] -WebSiteNames "Default Web Site" -ApplyECPAppPoolMitigation -ApplyOABAppPoolMitigation |

Các tham số có thể sử dụng để áp dụng biện pháp cụ thể:

- ApplyBackendCookieMitigation
- ApplyUnifiedMessagingMitigation

- ApplyECPAppPoolMitigation
- ApplyOABAppPoolMitigation

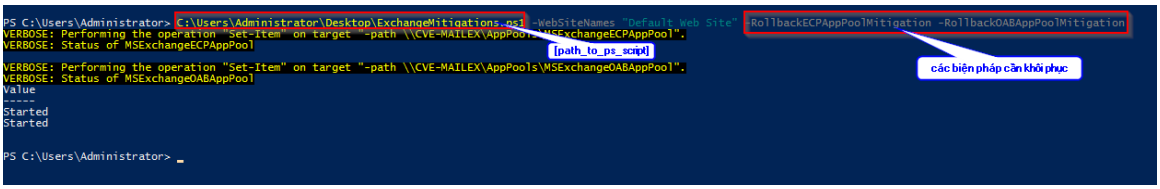



- Để khôi phục nhiều hoặc một biện pháp cụ thể, chạy câu lệnh sau:

```
[path_to_ps_script] -WebSiteNames "Default Web Site" -
RollbackECPAppPoolMitigation -RollbackOABAppPoolMitigation
```

Các tham số có thể sử dụng để áp dụng biện pháp cụ thể:

- RollbackBackendCookieMitigation
- RollbackUnifiedMessagingMitigation
- RollbackECPAppPoolMitigation
- RollbackOABAppPoolMitigation




- Để khôi phục tất cả các biện pháp, chạy câu lệnh sau:

```
[path_to_ps_script] -WebSiteNames "Default Web Site" -
RollbackAllMitigations
```

(Kết quả tương tự như trường hợp trên)