BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 61 /TTCNTT-KTHT
V/v lỗ hổng bảo mật trong Microsoft Exchange Server

Hà Nội, ngày 19 tháng 3 năm 2021

Kính gửi: Các đơn vị có hệ thống công nghệ thông tin trực thuộc Bộ

Ngày 02/3/2021, 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, chèn và thực thi mã từ xa (thông tin chi tiết về các lỗ hổng có tại phụ lục kèm theo).

Theo đánh giá sơ bộ của Cục An toàn thông tin rất nhiều máy chủ thư điện tử của Việt Nam (như máy chủ thư điện tử của cơ quan tổ chức nhà nước, tổ chức ngân hàng, tài chính, các doanh nghiệp và các tổ chức lớn khác) đang sử dụng Microsoft Exchange.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác minh hệ thống thông tin có khả năng bị ảnh hưởng bởi lỗ hổng trên để có phương án xử lý, khắc phục lỗ hổng. Quý đơn vị nên cập nhật, nâng cấp lên phiên bản mới nhất để khắc phục lỗ hổng bảo mật nói trên cũng như các lỗ hổng bảo mật mới phát hiện khác; đồng thời thực hiện tìm kiếm dấu hiệu tấn công theo hướng dẫn tại phụ lục kèm theo.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng. Đối với các cơ quan tổ chức có nhân sự kỹ thuật tốt có thể thử nghiệm xâm nhập vào hệ thống thông qua lỗ hổng này.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để biết);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
Thông tin về các lỗ hổng bảo mật trong Microsoft Exchange Server
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021)

1. 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) 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) Lỗi inseoure 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) 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) Cho phép đối tượng tấn công ghi file tùy ý sau xác thực.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065

2. 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

3. Hướng dẫn các bước phát hiện khả năng khai thác

Trong thời gian này, tạm thời chưa có các biện pháp để hạn chế và giảm thiểu nguy cơ tấn công của các lỗ hổng bảo mật này. Vì vậy, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị cập nhật lên phiên bản sớm nhất ngay khi có thể.

Ngoài ra, các quản trị viên có thể kiểm tra dấu hiệu khai thác bằng các bước sau:

1. CVE-3032-26855 có thể được phát hiện thông qua Exchange HttpProxy logs: %PROGRAMFILES%\Microsoft\ExchangeServer\V15\Logging\HttpProxy

Lệnh để tìm kiếm khả năng khai thác:

```
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
```

2. CVE-2021-26858 có thể được khai thác thông qua tệp Exchange log:

C:\Program Files\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog

Lệnh để tìm kiếm khả năng khai thác:

```
findstr /snip /c: "Download failed and temporary file"
"%PROGRAMFILES%\Microsoft\Exchange
Server\V15\Logging\OABGeneratorLog\*.log"
```

3. CVE-2021-26857 có thể được khai thác thông qua Windows Application event logs:

Source: MSExchange Unified Messaging

Entry Type: Error

Event Message Contains: System.InvalidCastException

Lệnh để tìm kiếm khả năng khai thác:

```
Get-EventLog -LogName Application -Source "MSExchange Unified Messaging" - EntryType Error | Where-Object { $_.Message -like "*System.InvalidCastException*" }
```

4. CVE-2021-27065 có thể phát hiện thông qua các tệp Exchange log:

C:\Program Files\Microsoft\Exchange Server\V15\Logging\ECP\Server

Lệnh PowerShell để tìm kiếm khả năng khai thác:

```
Select-String -Path "$env:PROGRAMFILES\Microsoft\Exchange Server\VI5\Logging\ECP\Server\*.log" -Pattern 'Set-. + VirtualDirectory'
```

4. Hướng dẫn kiểm tra các dấu hiệu cho thấy hệ thống đã bị khai thác

Quý đơn vị cần kiểm tra thêm các dấu hiệu sau nhằm phát hiện khả năng hệ thống thông tin đã bị khai thác như sau:

1. Dấu hiệu tấn công Authentication Bypass

- Kiểm tra IIS Log có truy cập tới các file sau:

```
/owa/auth/Current/themes/resources/logon.css
/owa/auth/CurrenEthemes/resources/owafont_ja.css
/owa/auth/Current/themes/resources/lgnbotl.gif
/owa/auth/Current/themes/resources/owafont_ko.css
/owa/auth/Current/themes/resources/SegoeUI-SemiBold.eot
/owa/auth/Current/themes/resources/SegoeUI-SemiLight.ttf
```

2. Dấu hiệu Webshell đã bị cài đặt trên hệ thống

```
\inetpub\wwwroot\aspnet_client\ (any .aspx file under this folder or sub folders)
\<exchange install path>\FrontEnd\HttpProxy\ecp\auth\ (any file besides TimeoutLogoff.aspx)
\<exchange install path>\FrontEnd\HttpProxy\owa\auth\ (any file or modified file that is not part of a standard install)
```

\<exchange install path>\FrontEnd\HttpProxv\owa\auth\Current\<any aspx file in this folder or subfolders>
\<exchange install path>\FrontEnd\HttpProxv\owa\auth\<folder with version number>\<any aspx file in this folder or subfolders>

3. Các User-Agents khả nghi trên Web log

DuckDuckBot/1.0;+(+http://duckduckgo.com/duckduckbot.html) facebookexternalhit/1.1+(+http://www.facebook.com/externalhit_uatext.php)
Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)
Mozilla/5.0+(compatible;+Bingbot/2.0;++http://www.bing.com/bingbot.htm)
Mozilla/5.0+(compatible;+Googlebot2.1;++http://www.google.com/bot.html
Mozilla/5.0+(compatible;+Konqueror/3.5;+Linux)+KHTML/3.5.5+(like+Gecko)+(Exabot-Thumbnails)
Mozilla/5.0+(compatible;+Yahoo!+Slurp;+http://help.yahoo.com/help/us/ysearch/slurp)
Mozilla/5.0+(compatible;+YandexBot/3.0;++http://yandex.com/bots)
Mozilla/5.0+(X11;+Linux+x86_64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/51.0.2704.103+Safari/537.36
ExchangeServicesClient/0.0.0.0
python-requests/2.19.1
python-requests/2.25.1
antSword/v2.1
Googlebot/2.1+(+http://www.googlebot.com/bot.html)
Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)

Ngoài ra, kiểm tra thêm các dấu hiệu tấn công mở rộng

1. Kiểm tra iis log có truy cập trả về mã 200 với đường dẫn

POST /owa/auth/Current/
POST /ecp/default.flt
POST /ecp/main.css
POST /ecp/<single char>.js

2. Kiểm tra các hệ thống có kết nối đến Exchange Server từ các IP:

STT	IP	STT	IP
1	103.77.192.219	9	192.81.208.169
2	104.140.114.110	10	203.160.69.66
3	104.250.191.110	11	211.56.98.146
4	108.61.246.56	12	5.254.43.18
5	149.28.14.163	13	5.2.69.14
6	157.230.221.198	14	80.92.205.81
7	167.99.168.251	15	91.192.103.43
8	185.250.151.72		

DANH SÁCH CÁC ĐƠN VỊ CÓ HỆ THỐNG CNTT

(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021)

STT	Tên đơn vị
1	Cục Thông tin khoa học và công nghệ quốc gia
2	Cục Sở hữu trí tuệ
3	Tổng cục Tiêu chuẩn Đo lường Chất lượng
4	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
5	Viện Năng lượng nguyên tử Việt Nam
6	Viện Khoa học sở hữu trí tuệ
7	Quỹ phát triển khoa học và công nghệ quốc gia
8	Cục An toàn bức xạ và hạt nhân
9	Quỹ đổi mới công nghệ quốc gia
10	Ban Quản lý Khu công nghệ cao Hòa Lạc