Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

# Nuevos días cero de Microsoft Exchange explotados activamente en ataques

*30/Septiembre/2022*

# Contenido

# INTRODUCCIÓN

Los actores de amenazas están explotando errores de día cero de Microsoft Exchange aún por revelar que permiten la ejecución remota de código, según afirman los investigadores de seguridad del equipo de ciberseguridad vietnamita GTSC, quienes detectaron e informaron por primera vez los ataques.

# Dia cero en Exchange

A continuación, se encuentra en cuadro de identificación de la amenaza.

| | |
|---|---|
| **ID de alerta:** | DSOC-CERT_2022_09_30_01 |
| **Clasificación de alerta:** | Vulnerabilidad |
| **Tipo de Impacto:** | ALTO |
| **TLP (Clasificación de información):** | **CLEAR** |
| **Fecha de publicación:** | 09/30/2022 |
| **Es día cero (0 day):** | Si |

## Resumen

Microsoft ha confirmado que dos vulnerabilidades de día cero informadas recientemente en Microsoft Exchange Server 2013, 2016 y 2019 se están explotando de forma salvaje.

"La primera vulnerabilidad, identificada como CVE-2022-41040, es una vulnerabilidad de falsificación de solicitud del lado del servidor (SSRF), mientras que la segunda, identificada como CVE-2022-41082, permite la ejecución remota de código (RCE) cuando PowerShell es accesible para el atacante", dijo Microsoft .

"En este momento, Microsoft está al tanto de ataques dirigidos limitados que utilizan las dos vulnerabilidades para ingresar a los sistemas de los usuarios".

La compañía agregó que la falla CVE-2022-41040 solo puede ser explotada por atacantes autenticados. La explotación exitosa les permite activar la vulnerabilidad CVE-2022-41082 RCE.

Microsoft dice que los clientes de Exchange Online no necesitan tomar ninguna medida en este momento porque la compañía cuenta con detecciones y mitigación para proteger a los clientes.

"Microsoft también está monitoreando estas detecciones ya implementadas en busca de actividad maliciosa y tomará las medidas de respuesta necesarias para proteger a los clientes. [...] Estamos trabajando en una línea de tiempo acelerada para lanzar una solución", agregó Microsoft.

Según el equipo de ciberseguridad vietnamita GTSC, quien fue el primero en informar sobre los ataques en curso , los días cero están encadenados para implementar shells web chinos Chopper para la persistencia y el robo de datos y para moverse lateralmente a través de las redes de las víctimas.

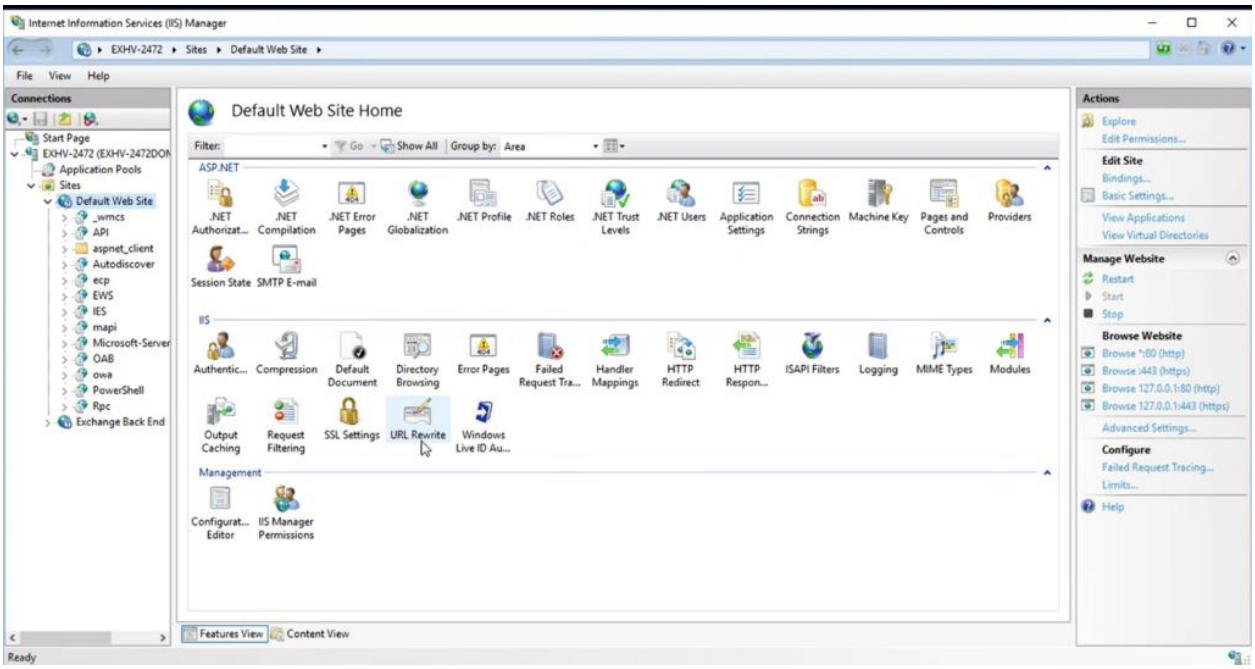
GTSC también sospecha que un grupo de amenazas chino podría ser responsable de los ataques en curso basados en la página de códigos de los shells web, una codificación de caracteres de Microsoft para el chino simplificado.

El grupo de amenazas también administra los shells web con la herramienta de administración de sitios web de código abierto chino Antsword, según lo revelado por el agente de usuario utilizado para instalarlos en servidores comprometidos.

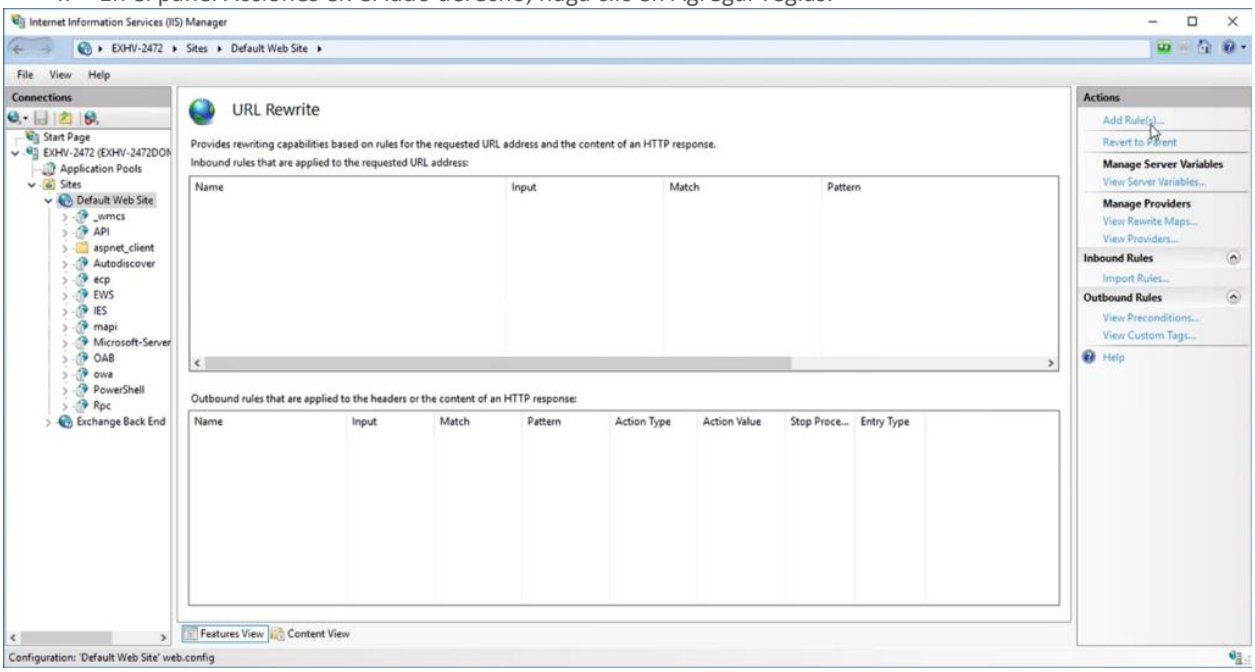
## Mitigación Disponible.

Los clientes de Microsoft Exchange Online no necesitan realizar ninguna acción. Los clientes locales de Microsoft Exchange deben revisar y aplicar las siguientes instrucciones de reescritura de URL y bloquear los puertos remotos de PowerShell expuestos.
La mitigación actual consiste en agregar una regla de bloqueo en "Administrador de IIS -> Sitio web predeterminado -> Reescritura de URL -> Acciones" para bloquear los patrones de ataque conocidos.
Microsoft ha confirmado que las siguientes instrucciones de reescritura de URL, que actualmente se están discutiendo públicamente, logran romper las cadenas de ataque actuales.

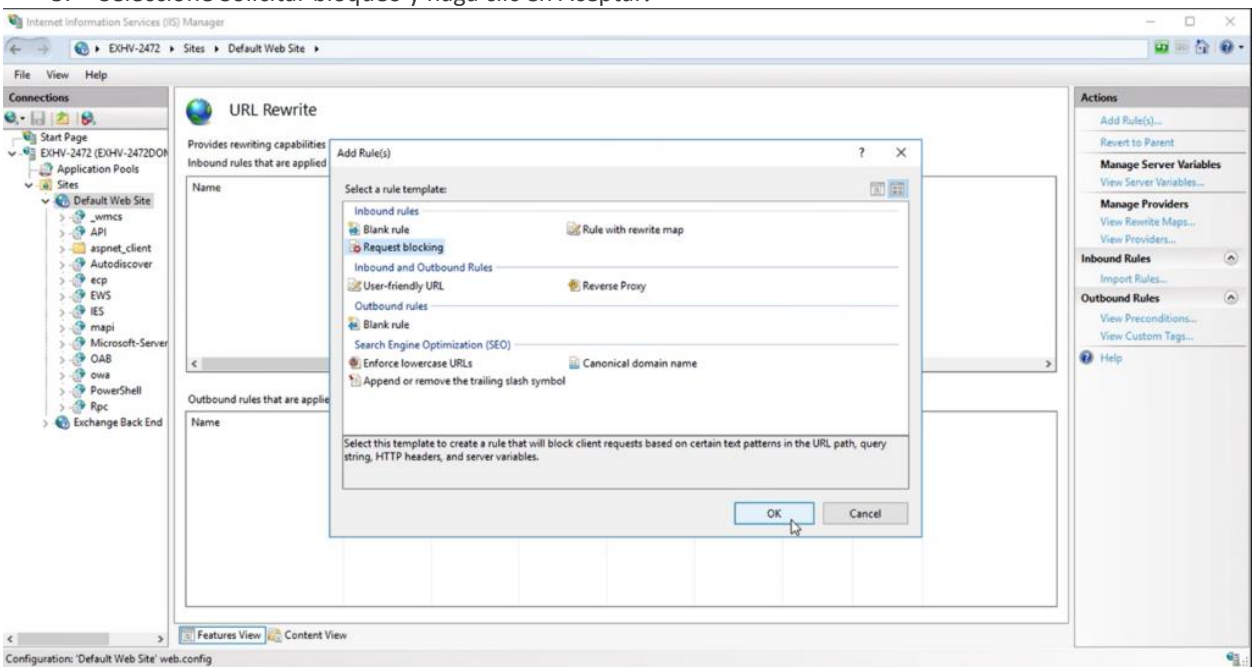
1. Abra el Administrador de IIS.
2. Expanda el sitio web predeterminado.
3. En la Vista de características, haga clic en Reescritura de URL.



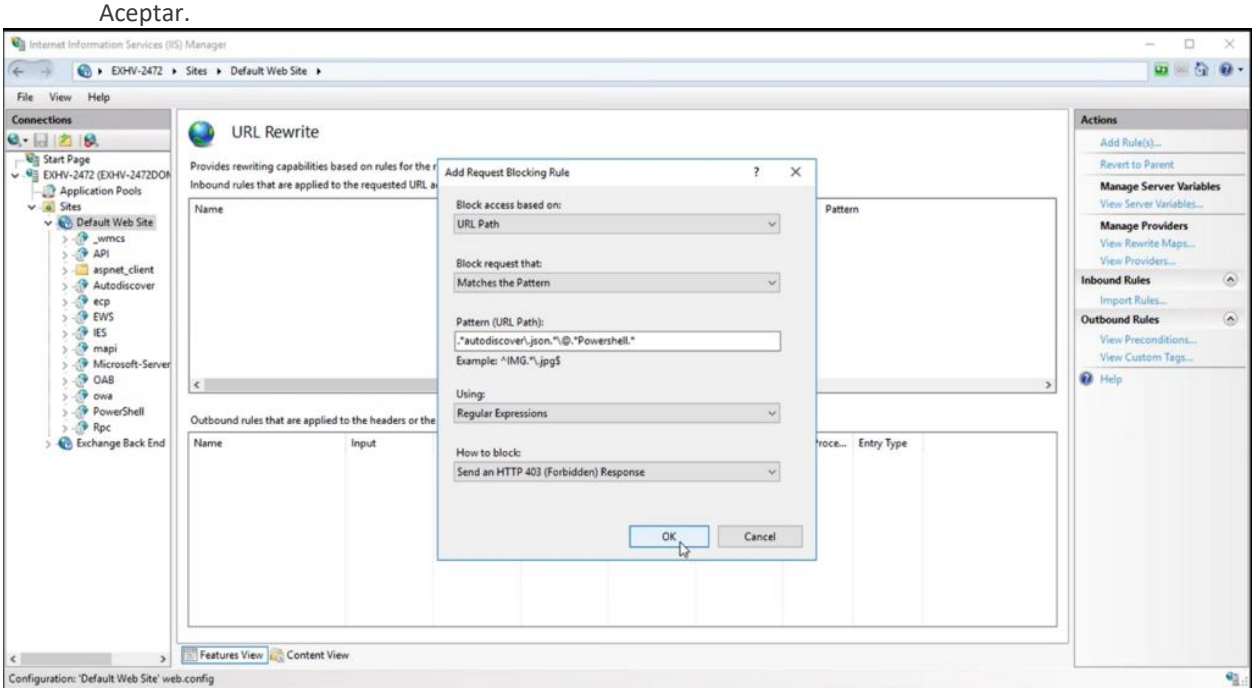
4. En el panel Acciones en el lado derecho, haga clic en Agregar reglas.



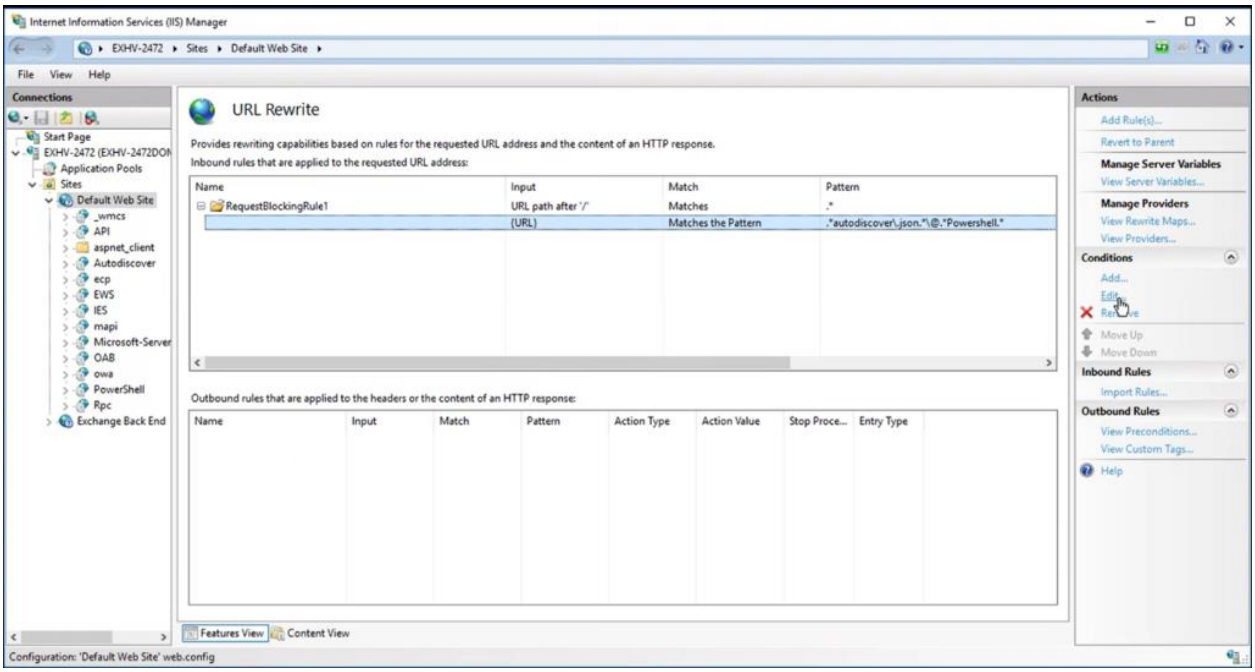

5. Seleccione Solicitar bloqueo y haga clic en Aceptar.



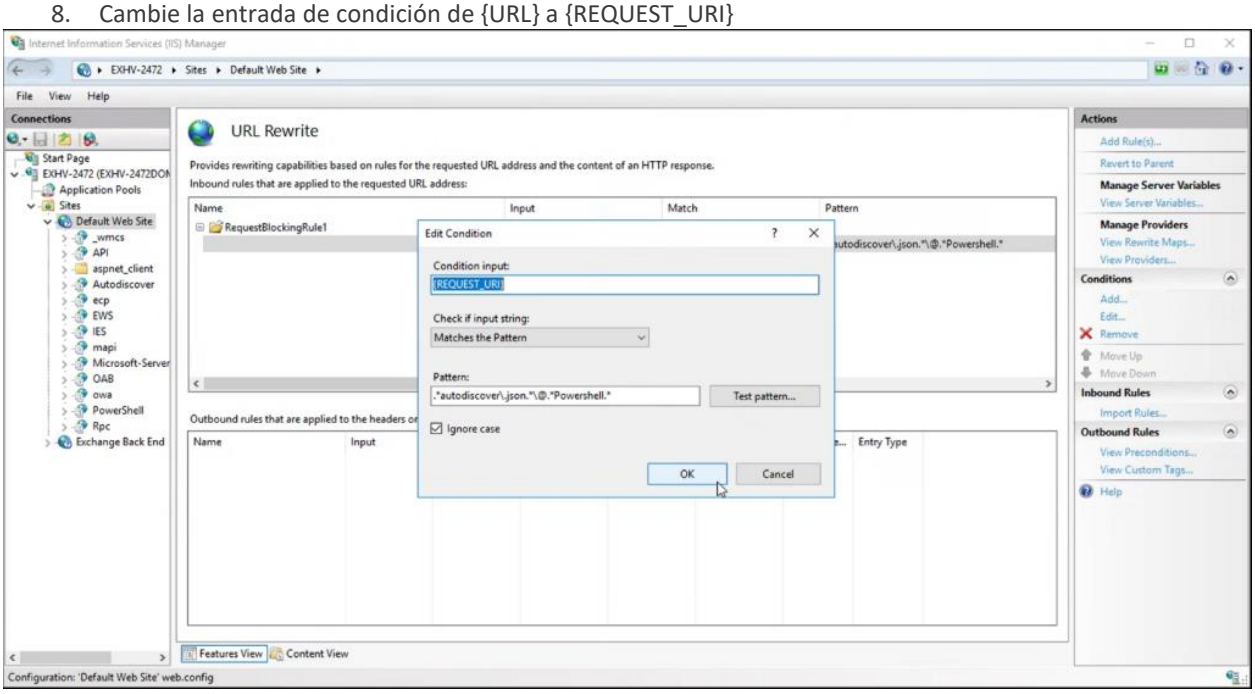
6. Agregue la cadena ".*autodiscover\.json.*\@.*Powershell.*" (excluyendo las comillas) y haga clic en Aceptar.




7. Expanda la regla y seleccione la regla con el Patrón ".*autodiscover\.json.*\@.*Powershell.*" y haga clic en Editar en Condiciones.



8. Cambie la entrada de condición de {URL} a {REQUEST_URI}




Impacto: no se conoce ningún impacto en la funcionalidad de Exchange si el módulo de reescritura de URL se instala según lo recomendado.
Los atacantes autenticados que pueden acceder a PowerShell Remoting en sistemas Exchange vulnerables podrán activar RCE mediante CVE-2022-41082. El bloqueo de los puertos utilizados para Remote PowerShell puede limitar estos ataques.

- HTTP: 5985
- HTTPS: 5986

GTSC dijo ayer que los administradores que deseen verificar si sus servidores de Exchange ya han sido comprometidos pueden ejecutar el siguiente comando de PowerShell para escanear los archivos de registro de IIS en busca de indicadores de compromiso:

```
Get-ChildItem -Recurse -Path <Path_IIS_Logs> -Filter "*.log" |
Select-String -Pattern
'powershell.*autodiscover\.json.*\@.*200'
```

# DETECCIONES

**Microsoft Defender para Endpoint**

Microsoft Defender para Endpoint detecta la actividad posterior a la explotación. Las siguientes alertas pueden estar relacionadas con esta amenaza:

- Posible instalación de shell web
- Posible shell web de IIS
- Ejecución de proceso de intercambio sospechoso
- Posible explotación de vulnerabilidades de Exchange Server
- Procesos sospechosos indicativos de un shell web
- Posible compromiso de IIS

Los clientes de Defender para Endpoint con Microsoft Defender Antivirus habilitado también pueden detectar el malware web shell utilizado en la explotación de esta vulnerabilidad en estado salvaje a partir de este escrito con las siguientes alertas:

- Se detectó malware 'Chopper' en un servidor web IIS
- Se detectó el malware de alta gravedad 'Chopper'

**Antivirus de Microsoft Defender Antivirus**

de Microsoft Defender detecta el malware posterior a la explotación utilizado en la explotación actual en estado salvaje de esta vulnerabilidad de la siguiente manera:

- Backdoor:ASP/Webshell.Y (Descripción de la amenaza Backdoor:ASP/Webshell.Y – Microsoft Security Intelligence)
- Backdoor:Win32/RewriteHttp.A (Descripción de la amenaza Backdoor:Win32/RewriteHttp.A – Microsoft Security Intelligence)

## Recomendaciones

- Se sugiere aplicar las mitigaciones mostradas en este documento para minimizar todo riesgo de exposición.

- Asegúrese de que sus servidores estén protegidos por software Antivirus y políticas de navegación adecuadas a nivel de firewall.

- Mantener monitoreo activo sobre todo tráfico sospechoso en red para poder realizar bloqueos a IPs no deseadas y sospechosas.

## Noticia Completa

https://devel.group/blog/dia-cero-en-exchange/

# CONTACTOS DE SOPORTE


**Correo electrónico:** cert@develsecurity.com

**Teléfonos directos:**

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

**Sitio Web:** https://www.devel.group/reporta-un-incidente