BOLETÍN DE ALERTA

Boletín Nro.: 2022-38
Fecha de publicación: 30/09/2022
Fecha de actualización: 10/11/2022
Tema: Vulnerabilidades de día cero en Microsoft Exchange Server - Actualización.
Actualizaciones:

- **07/10/2022:** se han realizado mejoras adicionales en la mitigación de la regla de reescritura de URL.
- **11/10/2022:** pasos 6 y 9 y las imágenes 8, 9 y 10.
- **02/11/2022:** se ha eliminado la opción de bloquear los puertos http/5985 y https/5986, se han agregado requisitos para explotación.
- **10/11/2022:** se han lanzado parches de actualizaciones para corregir las vulnerabilidades de día cero.

Algunos productos afectados son:

- Exchange Server 2013.
- Exchange Server 2016.
- Exchange Server 2019.

Descripción:

Microsoft ha informado sobre dos vulnerabilidades de día cero (*0-day*) que afectan a servidores de correo Microsoft Exchange Server, que permitirían a un atacante remoto realizar ataques del tipo *server-side request forgery* (*SSRF*) y ejecución remota de código (*RCE*). Actualmente para estas vulnerabilidades existen PoCs publicados en Internet.

- CVE-2022-41040, de severidad "Alta" y con puntuación asignada de 8.8. Esta vulnerabilidad de día cero (*0-day*) se debe a un error de control de acceso del servidor Exchange. Esto permitiría a un atacante remoto realizar ataques del tipo *server-side request forgery* (*SSRF*).

- CVE-2022-41082, de severidad "Alta" y con puntuación asignada de 8.8. Esta vulnerabilidad de día cero (*0-day*) se debe a una falla en el componente *PowerShell Handler*. Esto permitiría a un atacante realizar ejecución remota de código (*RCE*).

Estas vulnerabilidades requieren de una autenticación necesaria para la explotación de la CVE-2022-41040 y bastaría con una cuenta de usuario estándar, sin privilegios de administrador para iniciar la CVE-2022-41082. Las credenciales pueden ser obtenidas por el atacante a través de técnicas de phishing, ingeniería social, contraseñas comunes más utilizadas o adquiridas a través de filtraciones de credenciales.

Impacto:

La explotación exitosa de estas vulnerabilidades permitiría a un atacante ejecutar código de forma remota.

Detección:

Verificar si los servidores Microsoft Exchange han sido explotados:

1. Ejecutar el siguiente comando de PowerShell:

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

2. Verificar los archivos de registro del IIS a través de la herramienta NCSE0Scanner.

Solución:

Se recomienda acceder a las actualizaciones correspondientes a cada versión, provistas por el proveedor a través de los siguientes enlaces:

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

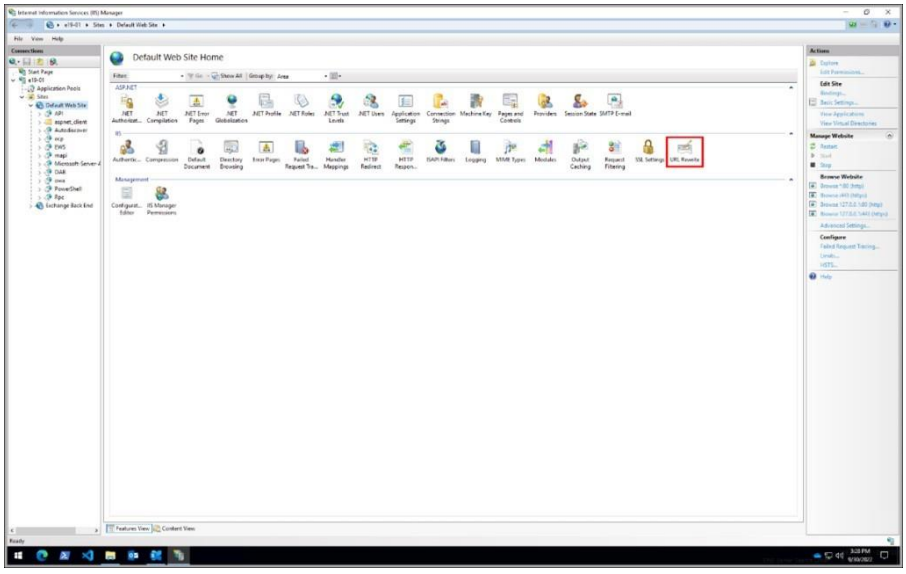
Mitigación:

En caso de no haber aplicado los parches correspondientes, es recomendable seguir los siguientes pasos de mitigación:

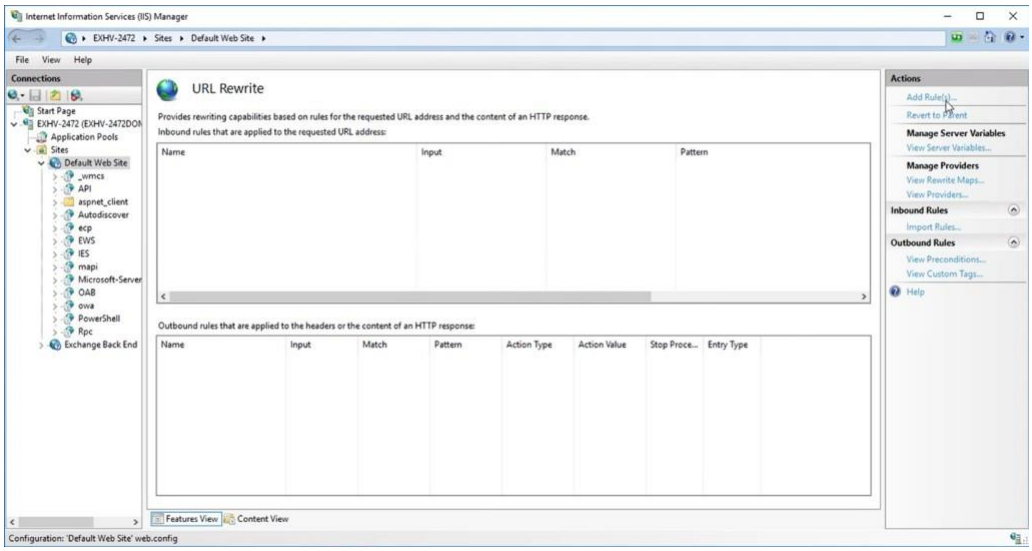
- Deshabilitar el acceso remoto a *PowerShell* para los usuarios que no sean administradores en su organización, a través del siguiente enlace.

- Si bien inicialmente *Microsoft* propuso como opción de mitigación bloquear los patrones de ataque conocidos a través de una regla en el *Administrador de IIS*, se encontró una manera de evadirla con poco esfuerzo, por lo que dicha regla actualmente se encuentra actualizada. Así también es posible ejecutar el script denominado *Exchange On-premises Mitigation Tool v2* para automatizar los pasos de reescritura de URL, o agregar la regla de reescritura de URL en el Administrador de IIS de manera manual, siguiendo los siguientes pasos:

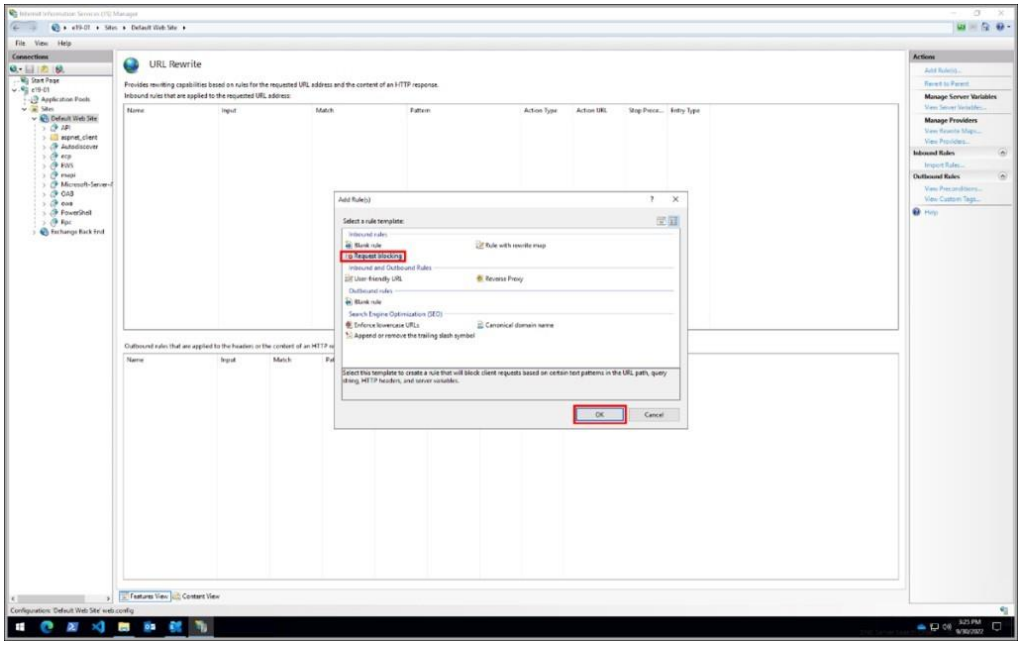
1. Abrir el Administrador de IIS.
2. Expandir el sitio Web predeterminado.
3. En la vista de características hacer clic en **Reescritura de URL**.



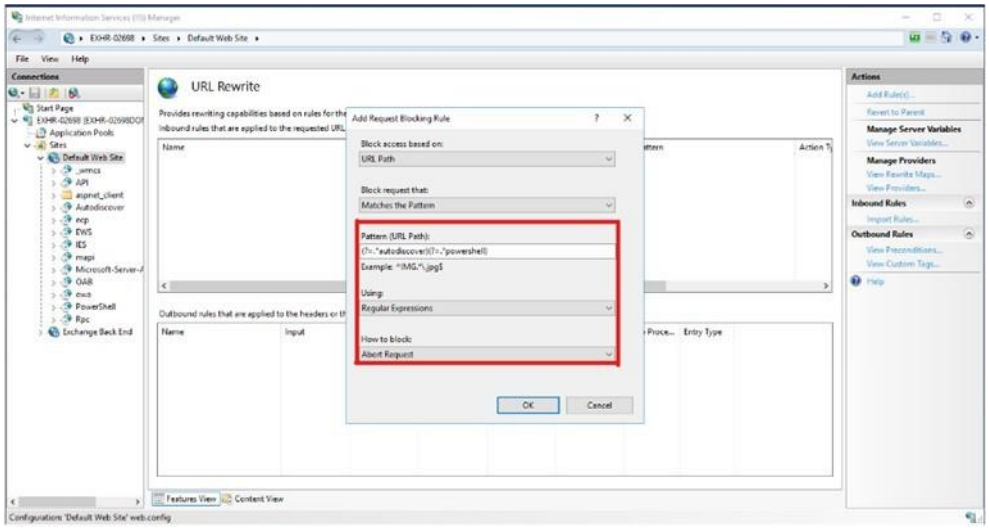
4. En el panel Acciones del lado derecho, hacer clic en **Agregar reglas**.



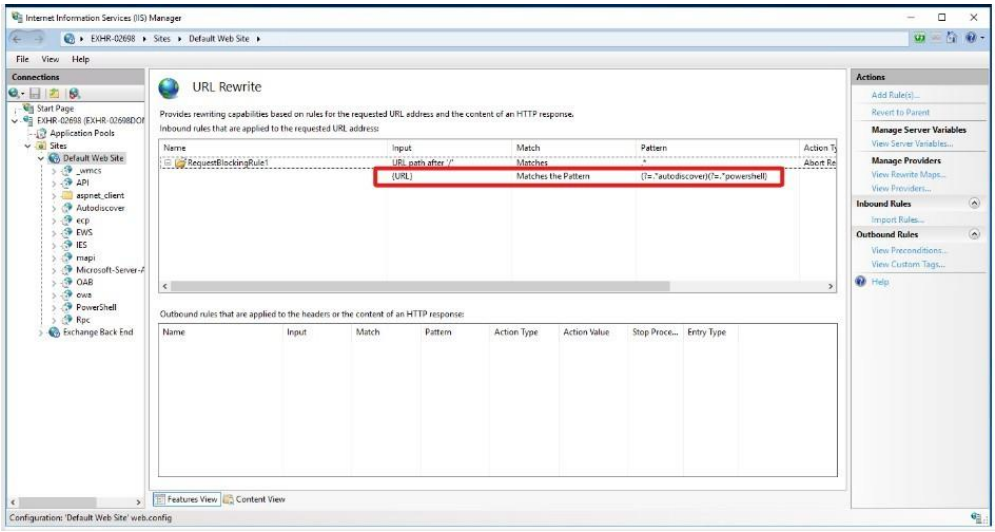
5. Seleccionar **Bloqueo de solicitudes** y hacer clic en **Aceptar**.



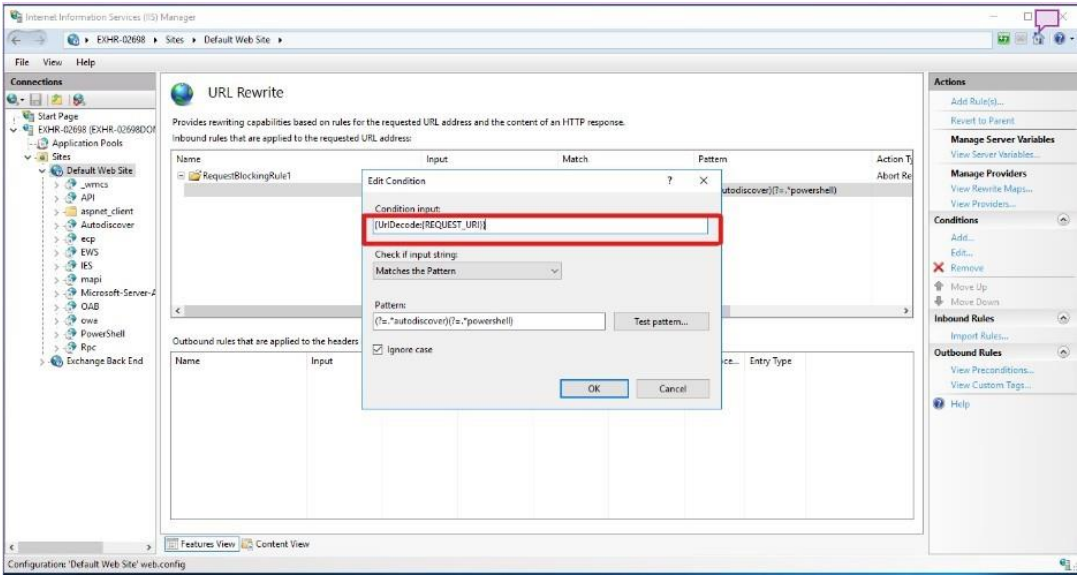
6. **Agregar** "(?=.*autodiscover)(?=.*powershell)".
7. Seleccionar la expresión regular en ***Using***
8. Seleccionar cancelar solicitud en ***How to block***, y luego hacer clic en **Aceptar**



9. Expandir la regla y seleccionar con el patrón (?=.*autodiscover)(?=.*powershell), y hacer clic en Editar en **Condiciones**.



10. Cambiar la entrada de condición de {URL} a {UrlDecode:{REQUEST_URI}}



Nota: Para clientes de Microsoft Exchange online, no se necesita realizar ninguna acción.

Una vez aplicadas las medidas de mitigación, puede comprobar si las mismas se aplicaron correctamente en su servidor de correo Microsoft Exchange, utilizando el siguiente script de nmap , escaneando la IP de su servidor de correo. El script no es oficial de Microsoft y fue publicado por un investigador de seguridad externo de confianza.

- https://github.com/CronUp/Vulnerabilidades/blob/main/proxynotshell_checker.nse

Si sospecha que su servidor haya podido quedar comprometido, puede utilizar como referencia el siguiente análisis de comportamiento malicioso publicado por el fabricante Microsoft

- https://www.microsoft.com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/

También puede utilizar como referencia el siguiente análisis publicado por un tercero:

- https://www.gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html

Información adicional:

- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/vulnerabilidades-0day-microsoft-exchange-server
- https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
- https://www.securityweek.com/microsoft-confirms-exploitation-two-exchange-server-zero-days
- https://www.gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html
- https://doublepulsar.com/proxynotshell-the-story-of-the-claimed-zero-day-in-microsoft-exchange-5c63d963a9e9
- https://www.rapid7.com/blog/post/2022/09/29/suspected-post-authentication-zero-day-vulnerabilities-in-microsoft-exchange-server/
- https://success.trendmicro.com/dcx/s/solution/000291651?language=en_US
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41040
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41082
- https://techcommunity.microsoft.com/t5/exchange-team-blog/released-november-2022-exchange-server-security-updates/ba-p/3669045

- https://www.microsoft.com/en-us/download/details.aspx?familyID=124eeb2b-4066-459e-9416-ee98683f4997
- https://www.microsoft.com/en-us/download/details.aspx?familyID=ddb4f351-5cb6-4ce4-93c1-ec6946f7c26a
- https://www.microsoft.com/en-us/download/details.aspx?familyID=09804a62-d5b7-4e38-9902-010326747aef