Basque CyberSecurity Centre

Vulnerabilidades zero-day en Microsoft Exchange

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

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 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:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Resumen ejecutivo

El equipo del Centro de Respuestas de Seguridad de Microsoft, ha realizado una publicación sobre dos vulnerabilidades de tipo zero-day que han sido reportadas inicialmente por el equipo de seguridad vietnamita conocido como GTSC.

La primera vulnerabilidad destacada por Microsoft está identificada bajo el CVE-2022-41040, que permite un ataque falsificación de solicitud del lado del servidor (SSRF). Sin embargo, el segundo error seguido bajo el CVE-2022-41082 da la posibilidad a un atacante remoto de ejecutar código arbitrario remotamente (RCE).

La compañía destaca el conocimiento que existe sobre la explotación de ambas vulnerabilidades, mencionando la necesidad de tener un acceso autenticado al servidor de Microsoft Exchange vulnerable. En los ataques dirigidos que aprovechan dichas vulnerabilidades, primeramente se ejecuta el error CVE-2022-41040, ya que permite a los atacantes aprovechar de manera remota el fallo descrito en el CVE-2022-410832.

Por el momento no se ha detectado la publicación de ningún exploit o pruebas de concepto (PoC) que aprovechen dichas vulnerabilidades.

Cabe añadir que por el momento no se ha llegado a aplicar una solución oficial que resuelva los errores descritos, pero tanto Microsoft como el GTSC han publicado mitigaciones alternativas. Desde el BCSC se recomienda aplicar las mismas con la mayor celeridad posible con el fin de tratar de evitar el compromiso de los sistemas vulnerables afectados por dichas vulnerabilidades, calificadas como críticas.

.

2. Análisis técnico

A consecuencia de su reciente descubrimiento, no existe por el momento información suficiente que permita conocer el detalle completo de las vulnerabilidades catalogadas bajo los CVE-2022-41040 y CVE-2022-41082 . A continuación, se destacan los detalles técnicos conocidos hasta el momento de ambos fallos:

- CVE-2022-41040: Vulnerabilidad que existe debido a la insuficiente validación de la entrada proporcionada por el usuario en la interfaz de Exchange OWA. Un usuario remoto puede enviar una solicitud HTTP especialmente diseñada y engañar a la aplicación para que inicie solicitudes a sistemas arbitrarios. La explotación exitosa de esta vulnerabilidad puede permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.
- CVE-2022-41082: Vulnerabilidad causada debido a una validación de entrada inadecuada. Un usuario remoto con acceso a PowerShell Remoting en sistemas Exchange vulnerables puede ejecutar código arbitrario.

En adición a lo anterior, GTSC ha dado a conocer tanto métodos de detección de posibles compromisos de los servidores de Exchange vulnerables, como los indicadores de compromiso (IOC´s) utilizados por los ciberatacantes que aprovechan las vulnerabilidades zero-day.

En relación a la búsqueda de un posible compromiso de un servidor, GTSC recomienda ejecutar el siguiente comando de PowerShell con la finalidad de escanear los archivos IIS en busca de indicadores de compromiso:

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

Los indicadores de compromiso (IOC´s) detectados en las vulnerabilidades descritas pueden consultar en el siguiente enlace:

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

Cabe destacar que tras el análisis de los mismos, se ha determinado que el origen de los atacantes que explotan dicha vulnerabilidad es asiático, ya que aplican webshells de Chopper.

Para finalizar, a continuación, se destacan los recursos afectados:

- Microsoft Exchange Server 2013, 2016 y 2019.

3. Mitigación / Solución

Como es habitual, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

Es importante que se tomen medidas rápidamente para mitigar este problema en la implementación. Por el momento, no se ha publicado un parche oficial, pero tanto Microsoft como GTSC han dado a conocer una mitigación alternativa que debe de ser aplicada.

Primeramente, Microsoft indica que aquellos usuarios que hagan uso de Microsoft Exchange Online no deben de realizar ninguna acción. Sin embargo, aquellas personas que usen Microsoft Exchange de manera local deben aplicar diversas instrucciones de reescritura de URL y bloquear los puertos remotos de PowerShell que han sido expuestos.

Para ello, los administradores deben añadir una regla de bloqueo en *"Administrador de ISS" > Sitio web predeterminado > Detección automática > Reescritura de URL > Acciones para bloquear los patrones de ataque conocidos*.

Tras llevar a cabo los pasos anteriormente indicados, dentro de la vista de características se debe entrar en *reescritura de URL*. Seguidamente se deben de añadir reglas en el panel de acciones presente. A continuación, solicitar el bloqueo, agregando la siguiente cadena:

- *.*autodiscover\.json.*\@.*Powershell.**

Tras realizar este paso, se debe expandir la regla anteriormente creada y editar las condiciones, cambiando la condición de entrada de *{URL}* a *{REQUEST_URI}*.

4. Referencias Adicionales

- Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server.
- Warning: New attack campaign utilized a new 0-day RCE vulnerability on Microsoft Exchange Server.
- MITRE: CVE-2022-41040.
- CWE-918: Server-Side Request Forgery (SSRF).
- MITRE: CVE-2022-41082.
- CWE-94: Improper Control of Generation of Code ('Code Injection').
- CWE-20: Improper Input Validation.
- Outlook en la web en Exchange Server.
- Connect to Exchange servers using remote PowerShell.
- https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html
- MITRE: China Chopper.

Basque CyberSecurity Centre

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?

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA