Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

TETÃ REKUÁI GOBIERNO NACIONAL

# BOLETÍN DE ALERTA

**Boletín Nro.**: 2021-04

**Fecha de publicación**: 03/02/2021

**Tema**: Vulnerabilidades críticas 0-day en Microsoft Exchange

**Sistemas afectados:**

- Microsoft Exchange 2013 (CU 23)
- Microsoft Exchange 2016 (CU 19, CU 18)
- Microsoft Exchange 2019 (CU 8, CU 7)

Obs.: Si bien, Exchange Server 2010 no es explotable, también ha sido incluido como una actualización de defensa en profundidad para Service Pack 3

**Descripción**

Se han descubierto 4 vulnerabilidades críticas de día 0 en Microsoft Exchange Server. Tres de ellas son de explotación remota (CVE-2021-26857, CVE-2021-26858 y CVE-2021-27065) y permiten la ejecución de código remoto; una de ellas, CVE-2021-26855, puede ser utilizada para obtener información sensible del servidor, pudiendo derivar en el robo de información de autenticación. Existe evidencia de que las 4 vulnerabilidades están siendo explotadas activamente en conjunto en el marco de ataques dirigidos. A continuación, se detallan las vulnerabilidades:

- CVE-2021-26855: vulnerabilidad del tipo server-side request forgery (SSRF) que permite al atacante enviar una petición HTTP arbitraria especialmente formada y autenticarse en el servidor
- CVE-2021-26857: vulnerabilidad de deserialización insegura en el servicio de mensaje unificado (Unified Messaging) que permite que datos no confiables y controlados por el usuario son deserializados por el servidor tal que permita la ejecución de código. En el caso de que el servicio se esté ejecutando con con privilegios de SYSTEM, el código se ejecutará con permisos de administración.
- CVE-2021-26858 y CVE-2021-27065: son vulnerabilidades de escritura arbitraria de archivos, posterior a la autenticación. Las mismas pueden ser explotadas de manera aislada luego de comprometer credenciales legítimas o en combinación con

CVE-2021-26855, sin necesidad de credenciales. Ambas pueden derivar en la ejecución remota arbitraria de código.

Los ataques observados por los investigadores en primer lugar, los atacantes logran el acceso al servidor Exchange a través de la explotación de la vulnerabilidad CVE-2021-26855. En algunos casos se observó que los atacantes utilizaron credenciales robadas previamente por otros medios. Seguidamente, combinando las vulnerabilidades CVE-2021-26857, CVE-2021-26858 y/o CVE-2021-27065, los atacantes crearon una webshell para controlar remotamente el servidor comprometido y de esta manera robar información de la red de la organización: libretas de contactos, buzones de correo, etc, base de datos del dominio, así como también información con miras al movimiento lateral a otros sistemas de la red. En algunos ataques se ha observado que los atacantes añadieron cuentas administrativas.

Microsoft ha publicado una actualización de emergencia que corrige las mencionadas vulnerabilidades. Exchange Online / Office 365 no está afectado, sin embargo, en caso de que cuente con una instancia on-premise, aunque sea solamente para administración, debe actualizarla. Para aplicar el parche de emergencia se debe asegurar que las actualizaciones acumulativas y de Rollup previas (Cumulative Update / Update Rollup - CU/RU)) ya estén instaladas.

**Impacto:**

La explotación combinada de algunas de las 4 vulnerabilidades mencionadas puede derivar en el control total del servidor Exchange por parte de un atacante remoto no autenticado.

**Solución y prevención**

- Instale las actualizaciones de Microsoft Exchange Server
- Puede utilizar el siguiente script para Nmap para escanear su red en busca de servidores potencialmente vulnerables: Nmap script (Autor: Kevin Beaumont)
    - Descargue el script, guardelo en /usr/share/nmap/scripts y ejecute el siguiente comando:
        - `nmap <rango_IP> -p<puerto> --script http-vuln-exchange`

- Para determinar si su servidor ha sido víctima de un ataque descrito en el presente boletín, puede seguir la siguiente guía de Microsoft para detectar indicadores de compromiso relevantes: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
    - En caso de detectar que su servidor fue comprometido, puede reportarlo a abuse@cert.gov.py para una investigación más profunda.

**Referencias**


- https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/
- https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901
- https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/