BOLETÍN DE ALERTA

Boletín Nro.: 2023-16
Fecha de publicación: 17/04/2023
Tema: Actualizaciones de seguridad para productos Microsoft

Principales softwares afectados son:

- Windows Server 2012 R2 (Server Core installation).
- Windows 10 Versión 1809 (ediciones de 32 y 64 bits).
- Windows 10 Versión 20H2 (ediciones de 32 y 64 bits).
- Windows 10 Versión 21H2 (ediciones de 32 y 64 bits).
- Windows Server 2016.
- Windows Server 2019.
- Windows Server 2008 - Server Core installation (ediciones de 32 y 64 bits).

Adicionalmente, puede acceder al listado completo de software afectado ingresando aquí.

Descripción:

Microsoft ha lanzado actualizaciones de seguridad sobre múltiples vulnerabilidades, incluyendo un Día Cero (*0-day*), que afectan a varios productos Microsoft, que permitirían a un atacante remoto realizar ejecución remota de código (*RCE*), divulgación de información, denegación de servicios (*DoS*), entre otros.

Las vulnerabilidades corregidas se componen de 7 (siete) de severidad "Crítica", 90 (noventa) de severidad "Alta", 2 (dos) de severidad "Media", 4 (cuatro) de severidad "Baja" y 21 (veintiuno) sin severidad asignada aún. Las principales que afectan al *MSMQ Service* se detallan a continuación:

- CVE-2023-21554, de severidad "Crítica" y con puntuación de 9.8. Esta vulnerabilidad se debe a una falla de limitación en Microsoft Message Queuing Server (*MSMQ Service*) de Windows. Esto permitiría a un atacante remoto a través del envío de paquetes *MSMQ* especialmente diseñados al servidor *MSMQ*, realizar escritura fuera de los límites y provocar ejecución remota de código (*RCE*) en el sistema afectado.
- CVE-2023-28252, de severidad "Alta" y con puntuación de 7.8. Esta vulnerabilidad de Día Cero (*0-day*) que está siendo explotada activamente se debe a una falla de límites en Windows Common Log File System (*CLFS*). Esto permitiría a un atacante local provocar corrupción de memoria y escalamiento de privilegios a *SYSTEM* en el sistema afectado.

- CVE-2023-21769 y CVE-2023-28302, ambas de severidad “Alta”, con una puntuación asignada de 7.5. Estas vulnerabilidades se deben a una falla de validación de datos de entrada del usuario en Microsoft Message Queue Server (*MSMQ Service*) de Windows. Esto permitiría a un atacante remoto a través del envío de comandos especialmente diseñados a la aplicación, realizar denegación de servicios (*DoS*) en el sistema afectado.

Adicionalmente, puede acceder al listado completo de vulnerabilidades ingresando aquí.

Impacto:

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante realizar ejecución remota de código (*RCE*), denegación de servicios (*DoS*), divulgación de información, escalamiento de privilegios, entre otros.

Solución:

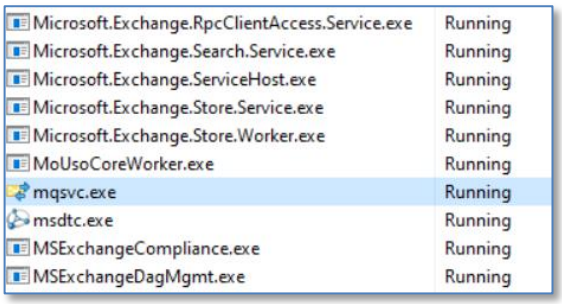
Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante a través de la siguiente guía:

- https://msrc.microsoft.com/update-guide

Mitigación:

Adicionalmente, como medida de mitigación para la vulnerabilidad CVE-2023-21554 se recomienda tener en cuenta los siguientes pasos:

1. Comprobar que el servicio *MSMQ* está instalado, en específico si existe un servicio en ejecución llamado Message Queuing Server y si el puerto *tcp 1801* está abierto en el equipo.



Fuente: https://research.checkpoint.com/2023/queuejumper-critical-unauthorized-rce-vulnerability-in-msmq-service/

2. Si se cuenta con dicho servicio instalado, verificar si su uso es necesario.
3. En caso de que su uso sea necesario y no se pueda instalar el parche de actualización, como solución temporal, recomendamos bloquear todas las conexiones entrantes al puerto *tcp 1801*.

Información adicional:

- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/actualizaciones-seguridad-microsoft-abril-2023
- https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2023-patch-tuesday-fixes-1-zero-day-97-flaws/
- https://research.checkpoint.com/2023/queuejumper-critical-unauthorized-rce-vulnerability-in-msmq-service/
- https://nvd.nist.gov/vuln/detail/CVE-2023-21554
- https://nvd.nist.gov/vuln/detail/CVE-2023-28252
- https://nvd.nist.gov/vuln/detail/CVE-2023-21769
- https://nvd.nist.gov/vuln/detail/CVE-2023-28302
- https://msrc.microsoft.com/update-guide
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21554
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28252
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21769
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28302
- https://www.cybersecurity-help.cz/vdb/SB2023041210
- https://www.cybersecurity-help.cz/vdb/SB2023041175
- https://www.cybersecurity-help.cz/vdb/SB2023041135