Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°175	Fecha: 25-07-2023
		Página: 4 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Las fallas críticas expusieron el servicio de Message Queuing de Microsoft a los ataques DoS		
Tipo de Ataque	Denegación de servicio DoS	Abreviatura	DoS
Medios de propagación	Red, Correo, Navegación de Internet		
Código de familia	F	Código de Sub familia	F01
Clasificación temática familia	Disponibilidad del Servicio		

Descripción

1. ANTECEDENTES:

Los investigadores del proveedor de soluciones de seguridad impulsadas por IA, FortiGuard Labs, han estado monitoreando el servicio Microsoft Message Queuing (MSMQ) durante los últimos meses. En un informe de investigación exclusivo, la compañía reveló detalles de múltiples vulnerabilidades de seguridad en el servicio de cola de mensajes ampliamente utilizado.

Las vulnerabilidades permiten la ejecución remota de código y ataques de denegación de servicio (ataques DoS), afectando principalmente a dispositivos basados en Windows con MSMQ instalado.

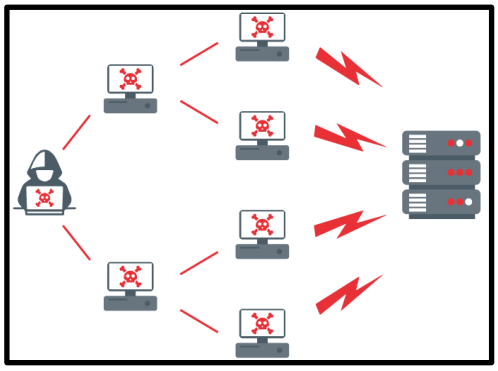
¿Qué es un Ataque de Denegación de Servicio (DoS)?

Es un tipo de ciberataque en el que un actor malicioso tiene como objetivo que un ordenador u otro dispositivo no esté disponible para los usuarios a los que va dirigido, interrumpiendo el funcionamiento normal del mismo. Los ataques DoS suelen funcionar al sobrecargar o inundar una máquina objetivo con solicitudes hasta que el tráfico normal es incapaz de ser procesado, lo que provoca una denegación de servicio a los usuarios de la adición. Un ataque DoS se caracteriza por utilizar un único ordenador para lanzar el ataque.

Un ataque de denegación de servicio distribuido (DDoS) es un tipo de ataque DoS que proviene de muchas fuentes distribuidas, como un ataque DDoS de una botnet.

Según Microsoft, los que intentan aplicar el ataque Denegación de Servicio, buscan principalmente causar interrupciones y generar publicidad. Se cree que emplean infraestructura de nube alquilada y redes privadas virtuales (VPN) para lanzar sus asaltos a los servidores de Microsoft, utilizando botnets compuestos por computadoras comprometidas de varios lugares del mundo.

Si bien los ataques DDoS generalmente se consideran molestias que hacen que los sitios web sean temporalmente inaccesibles sin infiltrarse en ellos, los expertos en el campo advierten que las interrupciones exitosas de un gigante de servicios de software como Microsoft pueden tener consecuencias de gran alcance, impactando el trabajo de millones y causando interrupciones en el comercio global



Denegación de Servicio

2. DETALLES:

Los detalles de cada defecto son los siguientes:

- **FG-VD-23-001: lectura fuera de los límites del encabezado de entrega exacta (EOD) de Message Queue Server**

  La falla permite la lectura fuera de los límites debido a que no se validan algunas funciones críticas, incluidas EodHeader, StreamIdSize y OrderQueueSize antes de que se acceda a ellas en la rutina del analizador del encabezado del mensaje (CQmPacket::CQmPacket).

  Los investigadores están de acuerdo en que este exploit de divulgación de información es inverosímil, pero los atacantes pueden lograr fácilmente un ataque de denegación de servicio si la lectura fuera de límite accede a una dirección no válida. FortiGuard Labs lanzó la firma MS.Windows.Message.Queuing.Service.CVE-2023-28302.DoS para detectar esta falla.

- **FG-VD-23-002: Escritura fuera de los límites del encabezado del mensaje de Message Queue Server**

  Cuando el analizador de encabezado de mensaje CQmPacket::CQmPacket no valida un encabezado de mensaje con un tamaño arbitrario, se produce una escritura fuera de límite.

  Un sondeo adicional reveló que algunos encabezados de mensajes, por ejemplo, EodHeader, EodAckHeader y CompoundMessageHeader, permiten a los atacantes especificar un tamaño/longitud arbitraria incorrectamente desinfectada si el analizador del encabezado del mensaje (que generalmente ajusta el puntero según las estructuras de datos predefinidas de cada encabezado) se ajusta para apuntar a una ubicación arbitraria.

  Esta sería una dirección no válida y puede causar daños en la memoria si el encabezado del mensaje se desreferencia más adelante en el código. Para detectar este problema, FortiGuard Labs lanzó la firma IPS MS.Windows.MSMQ.CVE-2023-21554.Remote.Code.Execution.

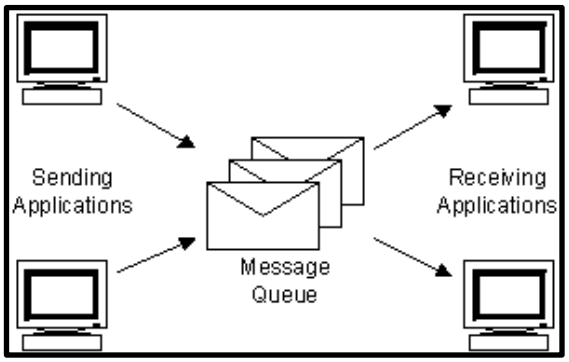
- **FG-VD-23-015: Escritura fuera de los límites del encabezado del mensaje compuesto de Message Queue Server**

  Este problema ocurre debido a una auditoría de código manual cuando el encabezado CompoundMessage no puede ejecutar una verificación de cordura en su estructura de datos.

¿Qué es MSMQ?

MSMQ es un servidor de Windows independiente alojado en MQSVC.EXE. Microsoft desarrolló este protocolo de mensajería patentado muy similar al RabitMQ de código abierto para que las aplicaciones que se ejecutan en diferentes computadoras puedan comunicarse de manera segura.

Los mensajes que no pueden llegar a su destino se colocan en una cola y se reenvían cuando se puede llegar al destino. El paquete MSMQ típico incluye encabezados como BaseHeader, UserHeader y MessagePropertiesHeader y también puede incluir TransactionHeader, SecurityHeader, DebugHeader y SessionHeader.



Microsoft Message Queuing

A. **Plataformas afectadas:** Windows.

B. **Partes afectadas:** Usuarios de Microsoft Windows con el servicio Microsoft Message Queuing instalado.

C. **Impacto:** Ejecución remota de código y denegación de servicio.

D. **Nivel de gravedad:** Crítico e importante.

3. RECOMENDACIONES:

- Identificar de inmediato los activos de red que presenten las vulnerabilidades mencionadas anteriormente y aplicar los parches y actualizaciones que Microsoft lanzó desde abril 2023.
- Implementar una política de Gestión de Parches, que se encargue de detectar, descargar, probar, aprobar e instalar parches nuevos o faltantes para todos los sistemas operativos y aplicaciones dentro de la red.

Fuente de Información:	• hxxps://www.hackread.com/microsoft-message-queuing-service-flaw-dos-attacks/ • hxxps://learn.microsoft.com/en-us/previous-versions/windows/desktop/msmq/ms711472(v=vs.85) • hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28302 • hxxps://www.fortiguard.com/zeroday/FG-VD-23-001 • hxxps://www.hackread.com/microsoft-ddos-attack-cyber-attack-impact/ • hxxps://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/#:~:text=Un%20ataque%20de%20denegaci%C3%B3n%20de%20servicio%20(DoS)%20es%20un%20tipo,el%20funcionamiento%20normal%20del%20mismo.

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°175**	**Fecha: 25-07-2023** **Página: 9 de 11**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en Ivanti Endpoint Manager Mobile		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **crítica** de tipo autenticación incorrecta en Ivanti Endpoint Manager Mobile (EPMM), anteriormente conocido como MobileIron Core. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto acceder a información confidencial y realizar cambios de configuración en el sistema vulnerable.

2. DETALLES:

La vulnerabilidad registrada con el código CVE-2023-35078 de severidad **crítica** de tipo autenticación incorrecta, permite el acceso no autenticado a rutas API específicas. Un atacante con acceso a estas rutas API puede acceder a información de identificación personal (PII), como nombres, números de teléfono y otros detalles de dispositivos móviles para usuarios en un sistema vulnerable. Un atacante también puede realizar otros cambios de configuración, incluida la creación de una cuenta administrativa de EPMM que puede realizar más cambios en un sistema vulnerable.

La vulnerabilidad de tipo autenticación incorrecta se da cuando un actor afirma tener una identidad dada, el producto no prueba o prueba insuficientemente que la afirmación es correcta.

A. Productos afectados:

- EPMM: 11.10, 11.9, 11.8 y 11.4;
- Versiones anteriores no compatibles también se ven afectadas.

3. RECOMENDACIÓN:

- Actualizar los productos afectados con la última versión de software disponible en el sitio web que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability?language=en_US • hxxps://nvd.nist.gov/vuln/detail/CVE-2023-35078 • hxxps://www.cisa.gov/news-events/alerts/2023/07/24/ivanti-releases-security-updates-endpoint-manager-mobile-epmm-cve-2023-35078