Boletín informativo
Vulnerabilidad en FortiClientEMS de Fortinet

CSIRTSALUD-AV-20260210-28 **TLP: CLEAR**

Incidente ID:	0028
Fecha del reporte:	10/02/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad en FortiClientEMS de Fortinet
Herramienta de detección	N/A
Activo involucrado:	Fortinet
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Medio

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la vulnerabilidad crítica (CVSSV3: 9.1) en FortiClientEMS de Fortinet, esta nueva vulnerabilidad fue identificada como CVE-2026-21643 la cual expone un fallo de inyección SQL en el componente GUI que permite a atacantes remotos no autenticados ejecutar código arbitrario o comandos no autorizados

Descripción:

Se ha identificado una vulnerabilidad de **Inyección SQL (CWE-89).** crítica en el servidor de **FortiClient Endpoint Management Server (EMS)**. Esta falla permite a un atacante no autenticado podría aprovechar **peticiones HTTP/HTTPS** específicamente manipuladas para ejecutar **código o comandos no autorizados**.

Se encuentra específicamente en el componente de **Interfaz Gráfica de Usuario (GUI)** del software. Debido a la falta de sanitización en los parámetros de entrada de ciertos endpoints del API, el atacante puede escalar privilegios o lograr la ejecución remota de comandos en el sistema operativo del servidor.

Cuando una SQLi alcanza este nivel de severidad, el riesgo va más allá de la base de datos: puede convertirse en un vector para toma de control, alteración de configuraciones, robo de información o incluso despliegue de malware en cadena.

Una explotación con éxito de CVE-2026-21643 puede derivar en:

- Ejecución de comandos en el servidor afectado.
- Acceso no autorizado a información y configuraciones.
- Alteración de la integridad de datos y políticas.
- Interrupción del servicio y degradación operativa.
- Riesgo de movimiento lateral hacia otros sistemas del entorno.

En escenarios reales, este tipo de fallo suele ser aprovechado para convertir una primera brecha en una intrusión persistente.

Productos afectados:

La vulnerabilidad afecta a las siguientes versiones de FortiClientEMS:

Producto	Versiones Afectadas
FortiClientEMS	Versiones 7.4

Modo de explotación y cadena de infección

La vulnerabilidad reside en el manejo de las peticiones que interactúan con el componente de base de datos de FortiClientEMS.

Mecanismo de explotación:

Acceso Inicial: El atacante no necesita credenciales válidas; solo requiere visibilidad de red hacia el puerto de administración del EMS (usualmente el 443 o el puerto configurado para la comunicación de endpoints). El atacante puede inyectar sentencias SQL que interactúan directamente con el motor de base de datos subyacente (usualmente Microsoft SQL Server).

Inyección: Se envía una carga útil (*payload*) a través de un campo vulnerable (frecuentemente en parámetros de filtrado o registro de dispositivos).

Escalada: La inyección permite no solo extraer o modificar datos de la base de datos, sino también escalar privilegios para lograr una **Ejecución Remota de Código (RCE)** en el sistema operativo del servidor utilizando funciones como xp_cmdshell.

Técnicas de Ataque (MITRE ATT&CK)

Los atacantes suelen seguir este patrón de comportamiento al explotar esta vulnerabilidad:

- **T1190 - Exploit Public-Facing Application:** Uso del exploit contra la interfaz web expuesta.

- **T1505.003 - Server Software Component: SQL Initial Access:** Obtención de acceso inicial mediante la base de datos.
- **T1059.001 - Command and Scripting Interpreter: PowerShell:** Una vez obtenido el RCE, se suelen desplegar scripts de PowerShell para descargar malware adicional o realizar persistencia.

Indicadores de compromiso:

En el momento Fortinet no ha reportado explotación activa de esta vulnerabilidad por lo que no se tienen indicadores de compromiso, por lo que Fortinet recomienda realizar acciones de monitorear los siguientes aspecto:

- **Logs de Red:** Solicitudes HTTP inusuales dirigidas a la interfaz de administración que contengan palabras clave SQL (e.g., UNION SELECT, WAITFOR DELAY, xp_cmdshell).

- **Procesos del Sistema:** Ejecución inesperada de cmd.exe o powershell.exe cuyo proceso padre sea FmcDaemon.exe o procesos relacionados con la base de datos de FortiClientEMS.

- **Conexiones Externas:** Intentos de conexión desde el servidor EMS hacia IPs externas no autorizadas inmediatamente después de tráfico administrativo anómalo.

Recomendaciones de mitigación:

Fortinet ha confirmado que las versiones de las ramas 8.0 y 7.2 **no están afectadas** por esta falla específica. Además, una actualización en la línea de tiempo el 6 de febrero de 2026 aclaró que las instancias de FortiEMS Cloud tampoco se ven afectadas, eliminando la preocupación inmediata para los clientes de SaaS.

La medida más efectiva es actualizar el producto a una versión corregida. La recomendación operativa es clara:

Actualiza FortiClientEMS a la versión 7.4.5 o superior.

Planifica la ventana de mantenimiento, pero no demorar la acción si el servicio está expuesto o es crítico para operaciones. Si tiene varias instancias (producción, preproducción, laboratorio), actualiza primero las más expuestas y después el resto.

Antes de ejecutar cualquier instalador, debes asegurar la recuperación en caso de falla:

- **Snapshot de VM:** Si el EMS está en una máquina virtual, toma un snapshot completo con la máquina apagada o en estado estable.

- **Respaldo de la Base de Datos:** Ve a Administration > Back up / Restore y genera un respaldo del archivo de configuración y de la base de datos SQL.
- **Verificación de Requisitos:** Confirma que el servidor cumple con los requisitos de hardware para la rama 7.4 (mínimo 4 vCPUs y 8 GB - 16 GB de RAM recomendados).

Descarga del Software

- Iniciar sesión en el portal de soporte de Fortinet (**support.fortinet.com**).
- Ir a **Support > Firmware Download**.
- Seleccionar **FortiClient** en la lista de productos.
- Navegar por las carpetas: FortiClient > Windows > EMS > v7.00 > 7.4 > 7.4.5.
- Descargar el ejecutable de instalación (ejemplo: FortiClientEMS_7.4.5.xxxx_x64.exe).

Proceso de Instalación (Upgrade)

El instalador de FortiClient EMS detectará automáticamente la versión anterior y realizará una actualización "in-place":

Post-Instalación y Verificación

Una vez finalizado el asistente:

- **Reinicio:** Se recomienda reiniciar el servidor para asegurar que todos los servicios y controladores se carguen correctamente.
- **Verificación de Servicios:** Abrir la consola de servicios de Windows (services.msc) y verificar que los servicios que inician con **"FortiClient EMS..."** estén en estado "En ejecución".
- **Consola Web:** Acceder a la GUI de administración y verifica en el Dashboard que la versión mostrada sea la **7.4.5**.
- **Sincronización de Endpoints:** Monitorear que los dispositivos (endpoints) comiencen a conectarse nuevamente y que no haya alertas de certificados.

Fuentes:

https://support.fortinet.com/welcome/#/
https://thehackernews.com/2026/02/fortinet-patches-critical-sqli-flaw.html
https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-de-inyeccion-sql-en-forticlientems-para-fortinet/
https://www.hkcert.org/security-bulletin/fortinet-forticlientems-remote-code-execution-vulnerability_20260210
https://fortiguard.fortinet.com/psirt/FG-IR-25-1142
https://nvd.nist.gov/vuln/detail/CVE-2026-21643
https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/CVE-2026-21643

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.