Alerta Vulnerabilidad
Vulnerabilidad Fortinet FortiClient EMS

CSIRTSALUD-AV-20260401-39

TLP: CLEAR

Incidente ID:	039
Fecha del reporte:	01/04/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad de Fortinet FortiClient EMS
Herramienta de detección	N/A
Activo involucrado:	Fortinet
Tipo de incidente:	Alerta de Vulnerabilidad
Nivel de riesgo:	Medio

Objetivo:

Informar a las entidades del Ecosistema y orientar a los equipos de ciberseguridad, administradores de red y gestores de riesgo sobre una vulnerabilidad crítica de inyección SQL identificada en Fortinet FortiClient Endpoint Management Server (EMS), registrada bajo el identificador CVE-2026-21643.

Dado que se ha confirmado explotación activa en entornos reales desde el 26 de marzo de 2026, este documento proporciona información técnica detallada para facilitar la detección, contención y remediación de la amenaza de forma inmediata.

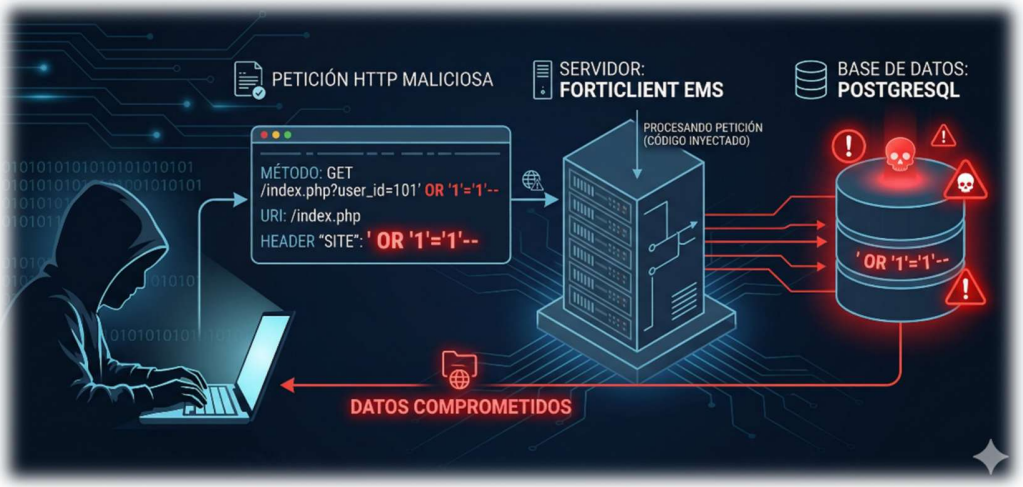
Descripción:

FortiClient EMS es una plataforma de administración centralizada que permite a las organizaciones desplegar, configurar y supervisar los agentes FortiClient en múltiples endpoints a través de su interfaz web HTTPS. También admite implementaciones multi-tenant, lo que permite gestionar múltiples sitios de clientes desde una sola instancia.

Alerta Vulnerabilidad
Vulnerabilidad Fortinet FortiClient EMS

CSIRTSALUD-AV-20260401-39 **TLP: CLEAR**

La vulnerabilidad CVE-2026-21643 es una falla de inyección SQL (SQL Injection) causada por la neutralización inadecuada de elementos especiales en los comandos SQL procesados por la interfaz gráfica (GUI) web de FortiClient EMS. El defecto fue introducido en la versión 7.4.4 durante una refactorización de la capa middleware y de conexión de base de datos para soportar la funcionalidad multi-tenant mejorada.



El vector de ataque es directo: un atacante remoto no autenticado puede enviar peticiones HTTP especialmente diseñadas a la interfaz administrativa del servidor EMS expuesta a internet y ejecutar consultas SQL arbitrarias sobre la base de datos PostgreSQL subyacente, con la posibilidad de escalar hasta la ejecución de código o comandos en el sistema operativo del servidor.

La explotación exitosa de esta vulnerabilidad puede derivar en las siguientes consecuencias de alto impacto:

- Ejecución remota de código (RCE): El atacante puede ejecutar comandos arbitrarios en el sistema operativo del servidor EMS, tomando control total del mismo.
- Extracción de credenciales administrativas: Acceso a cuentas de administración almacenadas en la base de datos, permitiendo el movimiento lateral hacia otros sistemas gestionados.
- Robo de datos sensibles: Exposición del inventario de endpoints, políticas de seguridad, certificados de los dispositivos gestionados y configuraciones de red.
- Pivot hacia la red interna: Dado que EMS gestiona todos los endpoints, un atacante podría utilizar este servidor como punto de entrada para infiltrarse en la red corporativa.
- Distribución de malware: Uso del servidor EMS comprometido para desplegar cargas maliciosas (ransomware, spyware, etc.) en los endpoints gestionados.
- Interrupción del servicio: Modificación o eliminación de políticas de seguridad y configuraciones, afectando la disponibilidad del servicio de gestión de endpoints.
- Persistencia avanzada: Creación de backdoors o cuentas ocultas que permitan acceso continuo incluso tras la aplicación del parche.

Modo de explotación y cadena de infección

La versión 7.4.4 de FortiClient EMS introdujo soporte mejorado para despliegues multi-tenant. Como parte de esta funcionalidad, cada solicitud HTTP al servidor incluye un header personalizado llamado 'Site' que identifica a qué tenant pertenece la petición. El error crítico radica en que este header es tomado directamente del request HTTP y concatenado en una consulta SQL hacia la base de datos PostgreSQL sin ningún proceso de sanitización o validación de entrada, y —lo más grave— este procesamiento ocurre ANTES de que cualquier mecanismo de autenticación sea verificado.

A continuación se describe la cadena de explotación completa de CVE-2026-21643:

Reconocimiento

- El atacante identifica instancias de FortiClient EMS expuestas en internet utilizando motores de búsqueda de dispositivos como Shodan o Censys con queries como: product:"FortiClientEMS".
- Verifica que la versión sea 7.4.4 revisando las cabeceras HTTP de respuesta, mensajes de error o páginas de login que revelen información de versión.
- Confirma la accesibilidad de la interfaz web HTTPS en el puerto 443 (o puerto alternativo configurado).

Exploración y Validación de la Inyección

El atacante envía una solicitud HTTP de prueba al endpoint vulnerable para confirmar la existencia de la falla:

```
POST /api/v1/init_consts HTTP/1.1
Host: <TARGET_EMS_IP>
Content-Type: application/json
Site: x'; SELECT pg_sleep(5)--
...
```

Si el servidor tarda ~5 segundos en responder (tiempo-based blind SQLi), confirma la vulnerabilidad. Este método de 'time delay' es el más silencioso y menos propenso a generar alertas.

Extracción de Datos

Una vez confirmada la inyección, el atacante puede exfiltrar información sensible de la base de datos PostgreSQL mediante técnicas de blind SQL injection o error-based SQL injection:

- Enumeración de la estructura de la base de datos (tablas, columnas).
- Extracción de hashes de contraseñas de cuentas administrativas.
- Obtención de tokens de sesión activos y certificados digitales de endpoints.
- Lectura de archivos del sistema operativo mediante funciones PostgreSQL como pg_read_file().

Escalada a Ejecución de Código Remoto

PostgreSQL permite ejecutar comandos del sistema operativo utilizando la instrucción COPY ... FROM PROGRAM, que el atacante puede invocar a través de la inyección:

```
Site: x'; COPY cmd_out FROM PROGRAM 'id' --
```

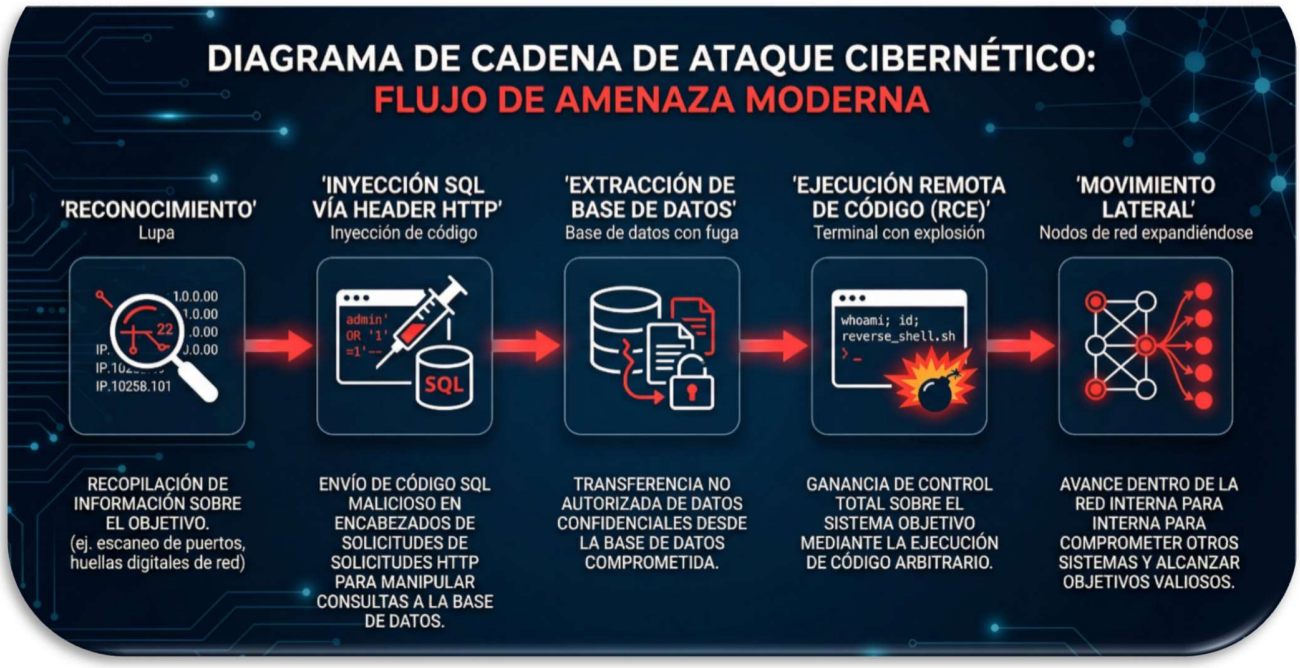
Esto permite escalar desde la inyección SQL a ejecución arbitraria de comandos en el servidor, logrando control total del sistema. A partir de aquí, el atacante puede:

- Descargar e instalar herramientas de post-explotación (implantes, C2 beacons).
- Crear cuentas de backdoor en el sistema operativo y en FortiClient EMS.
- Moverse lateralmente hacia endpoints gestionados.
- Desplegar ransomware o herramientas de espionaje a través de la consola de gestión EMS.

Alerta Vulnerabilidad
Vulnerabilidad Fortinet FortiClient EMS

CSIRTSALUD-AV-20260401-39

TLP: CLEAR



A continuación se detalla la vulnerabilidad explotada:

Atributo	Detalle
Tipo de falla	Improper Neutralization of Special Elements in SQL Commands (CWE-89)
Vector de acceso	Red (remoto) — AV:N
Complejidad	Baja — AC:L
Privilegios requeridos	Ninguno — PR:N

CSIRT Salud

Alerta Vulnerabilidad
Vulnerabilidad Fortinet FortiClient EMS

CSIRTSALUD-AV-20260401-39

TLP: CLEAR

Atributo	Detalle
Interacción de usuario	No requerida — UI:N
Alcance	Sin cambio — S:U
Impacto Confidencialidad	Alto — C:H
Impacto Integridad	Alto — I:H
Impacto Disponibilidad	Alto — A:H
Vector CVSS 3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Puntuación	9.8 — CRÍTICO
Causa raíz	El header HTTP 'Site' es concatenado directamente en una query SQL sin sanitización, antes de cualquier verificación de autenticación

Relación con tácticas MITRE ATT&CK

La explotación de CVE-2026-21643 se alinea con las siguientes tácticas y técnicas del marco MITRE ATT&CK for Enterprise:

Táctica	ID Técnica	Nombre	Descripción de aplicación
Acceso Inicial	**T1190**	Exploit Public-Facing Application	El atacante explota la interfaz web de FortiClient EMS accesible desde internet sin autenticación.

CSIRT Salud

Alerta Vulnerabilidad
Vulnerabilidad Fortinet FortiClient EMS

CSIRTSALUD-AV-20260401-39

TLP: CLEAR

Táctica	ID Técnica	Nombre	Descripción de aplicación
Ejecución	**T1059**	Command and Scripting Interpreter	Uso de funciones PostgreSQL (COPY FROM PROGRAM) para ejecutar comandos del SO.
Persistencia	**T1136**	Create Account	Creación de cuentas administrativas de backdoor en el sistema EMS comprometido.
Escalada de privilegios	**T1068**	Exploitation for Privilege Escalation	Escalada desde usuario de base de datos a privilegios de sistema operativo.
Evasión de defensa	**T1562**	Impair Defenses	Modificación de políticas de seguridad de endpoints gestionados por EMS.
Acceso a credenciales	**T1552**	Unsecured Credentials	Extracción de hashes de contraseñas y certificados desde la base de datos.
Descubrimiento	**T1018**	Remote System Discovery	Enumeración del inventario completo de endpoints gestionados por EMS.
Movimiento lateral	**T1210**	Exploitation of Remote Services	Uso del servidor EMS comprometido para pivotar hacia los endpoints gestionados.
Exfiltración	**T1041**	Exfiltration Over C2 Channel	Transferencia de datos sensibles hacia infraestructura controlada por el atacante.
Impacto	**T1486**	Data Encrypted for Impact	Despliegue de ransomware en endpoints a través de la consola de gestión EMS.

Activos o versiones afectados:

La vulnerabilidad afecta de forma específica y exclusiva a la siguiente versión del producto:

Versión FortiClient EMS	¿Afectada?	Solución
8.0 y superior	NO AFECTADA	No aplica

Alerta Vulnerabilidad
Vulnerabilidad Fortinet FortiClient EMS

CSIRTSALUD-AV-20260401-39

TLP: CLEAR

Versión FortiClient EMS	¿Afectada?	Solución
7.4.4	SÍ — CRÍTICO	Actualizar a 7.4.5 o superior
7.4.3 e inferior	NO AFECTADA	No aplica
7.2.x	NO AFECTADA	No aplica

La vulnerabilidad requiere que el servidor FortiClient EMS esté configurado en modo multi-tenant (introducido en versiones anteriores a 7.4.4 pero potenciado en esta versión). Las instancias con la interfaz web accesible directamente desde internet son las de mayor riesgo inmediato.

Indicadores de compromiso:

Indicadores de Red

- IP de ataque documentada: 104.192.92[.]135 (observada en payload activo de explotación).
- Solicitudes HTTPS inusuales hacia el endpoint /api/v1/init_consts del servidor FortiClient EMS.
- Presencia del header HTTP 'Site' con valores sospechosos o contenido SQL (p. ej. x'; SELECT pg_sleep(4)--).
- Tráfico HTTPS desde direcciones IP no pertenecientes a rangos administrativos aprobados.

Indicadores en Logs del Servidor

- Entradas en logs web con headers 'Site' que contengan caracteres especiales SQL: comillas simples ('), punto y coma (;), doble guion (--).

- Consultas SQL inesperadas en logs de la base de datos PostgreSQL, especialmente funciones como pg_sleep(), pg_read_file(), COPY TO/FROM PROGRAM.
- Errores de base de datos relacionados con sintaxis SQL inválida correlacionados con peticiones HTTP externas.
- Accesos al panel de administración EMS desde fuera del horario habitual o desde geografías inusuales.

Indicadores en el Sistema

- Creación de cuentas administrativas no autorizadas en FortiClient EMS.
- Cambios en políticas de seguridad de endpoints sin justificación.
- Presencia de herramientas de post-explotación (webshells, reverse shells, etc.) en el directorio de instalación del servidor EMS.
- Procesos hijos inusuales lanzados desde el proceso del servidor EMS.

Recomendaciones de mitigación:

- Actualizar FortiClient EMS a la versión 7.4.5 o superior de forma inmediata. El parche fue liberado el 6 de febrero de 2026.

- Restringir el acceso a la interfaz web de administración de FortiClient EMS. Eliminar la exposición directa a internet y permitir acceso únicamente desde redes internas de confianza o a través de VPN corporativa.

- Implementar reglas de firewall perimetral para bloquear conexiones entrantes no autorizadas al puerto de administración del servidor EMS (usualmente TCP/443).

- Desplegar reglas de detección de SQL Injection en el sistema de prevención de intrusiones para el tráfico HTTPS dirigido al servidor EMS. Habilitar inspección SSL/TLS en el IDS para analizar el contenido de peticiones cifradas.

- Auditoría de base de datos: Habilitar el log de consultas en PostgreSQL para detectar instrucciones inusuales como pg_sleep(), COPY FROM PROGRAM, o consultas sobre tablas de sistema de autenticación.

Fuentes:

- CISA — Known Exploited NVD — National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2026-21643
- Fortinet PSIRT Advisory: https://www.fortiguard.com/psirt
- BleepingComputer: Critical Fortinet FortiClient EMS flaw now exploited in attacks (30/03/2026)
- Help Net Security: Critical Fortinet FortiClient EMS bug under active attack (30/03/2026)
- SOC Prime Blog: CVE-2026-21643 (10/02/2026)
- Arctic Wolf: CVE-2026-21643 Analysis (09/02/2026)
- SecPod Blog: FortiClient EMS Under Fire (31/03/2026)

- MITRE ATT&CK Framework: https://attack.mitre.org
- Shadowserver Foundation: Internet-exposed FortiClient EMS tracking

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.