Alerta

Técnica

Vulnerabilidades identificadas en Fluent Bit

COLCERT AL-20251127 - 085

TLP:CLEAR

Resumen Ejecutivo

Fluent Bit es un agente ampliamente utilizado para la recolección y transporte de *logs* en infraestructuras empresariales y en la nube, crítico para la visibilidad y detección de incidentes. Las vulnerabilidades recientemente identificadas exponen fallas que permiten manipulación de logs, lectura o escritura no autorizada de archivos, alteración de evidencias y desvío de telemetría, comprometiendo la confiabilidad del monitoreo.

Dado su despliegue masivo, existe una alta probabilidad de que organizaciones dependientes de **Fluent Bit** sean impactadas si no aplican medidas de mitigación. A futuro, es muy probable que actores maliciosos incorporen estos vectores de compromiso en campañas dirigidas para afectar la integridad de los sistemas de detección. Esto incrementa el riesgo de ceguera operacional y retrasos en la respuesta ante incidentes, lo cual exige decisiones proactivas de actualización, endurecimiento y revisión de arquitectura de *logging*.

NIVEL DE RIESGO

ALTO

Vulnerabilidades identificadas

CVE	Producto afectado	Descripción	Score CVSS
CVE-2025-12972	Plugin out_file (salida a archivos)	Permite inyectar en el tag valores con ../ y escribir archivos arbitrarios fuera del directorio previsto. Permite RCE si Fluent Bit corre con permisos elevados.	5.3 (Medio)
CVE-2025-12970	Plugin in_docker (input desde Docker)	Un nombre de contenedor demasiado largo puede corromper memoria, con posibilidad de Denegación de Servicio (DoS) o ejecución remota de código (RCE).	8.8 (Alto)
CVE-2025-12969	Plugin in_forward (input de logs “forwarded”)	Permite a atacantes remotos enviar datos sin credenciales si la configuración no es correcta. Pueden inyectar logs falsos, saturar alertas, manipular flujos.	6.5 (Medio)
CVE-2025-12977	Plugins in_http, in_splunk, in_elasticsearch (input HTTP / Splunk / Elastic)	Permite inyección de etiquetas maliciosas (tags con nuevos saltos de línea, ../, etc.), *log tampering*, redirección o manipulación de logs.	**9.1 (Crítico)**
CVE-2025-12978	Mismos plugins que arriba	Permite *spoofing* parcial de etiquetas, manipulación de *routing* de *logs*, posible redirección a destinos no autorizados o filtración.	5.4 (Medio)

¿Cómo los ciberdelincuentes pueden explotar estas vulnerabilidades en Fluent Bit?

Los actores maliciosos pueden aprovechar estas fallas en Fluent Bit manipulando los componentes que procesan entradas externas (*input plugins*) o que manejan datos no confiables. Estas vulnerabilidades permiten enviar peticiones especialmente diseñadas, capaces de alterar el flujo normal del agente de *logging*. En términos generales, los ciberdelincuentes pueden explotar estas debilidades mediante:

1. **Envío de datos malformados o manipulados a los *plugins* de entrada**: Plugins como *in_http*, *in_forward*, *in_docker* y *in_elasticsearch* aceptan datos desde fuentes externas. Un atacante puede enviar peticiones construidas para activar errores de validación, desbordamientos o saltos lógicos, desencadenando la ejecución inesperada de código, manejo incorrecto de etiquetas (tags) y denegación de servicio del agente.

2. **Aprovechamiento de fallas en la sanitización de campos**: algunas vulnerabilidades se activan modificando valores en campos que **Fluent Bit** espera que sean benignos. Los actores pueden inyectar contenido malicioso dentro de los campos procesados, logrando cambiar la ruta o el destino de los logs, manipular cómo se clasifican o enrutan los eventos, ocultar su actividad alterando el *pipeline* de telemetría.

3. **Manipulación de metadatos enviados desde contenedores o servicios integrados**: en escenarios con Docker o Kubernetes, un atacante con acceso limitado a un contenedor puede modificar metadatos o nombres de entidades, lo que activa fallas como desbordamientos de memoria o errores en el parseo. Esto les permite afectar el funcionamiento del agente desde niveles bajos.

4. **Exposición de endpoints de ingesta sin controles de acceso:** estas fallas permiten que un atacante se conecte a los puertos de ingesta disponibles y envíe datos maliciosos o manipulados, alterando flujos, activando parsers no deseados o inyectando contenido en los pipelines de monitoreo.

5. **Forzar escritura en ubicaciones no destinadas**: cuando existe una debilidad en los *plugins* de salida, un actor de amenaza puede manipular rutas de archivos para inducir a **Fluent Bit** a escribir contenido en áreas no autorizadas. Esto puede utilizarse para sobrescribir archivos legítimos, generar registros falsificados, sabotear la operación de otros servicios en el sistema.

Aunque las técnicas anteriores varían según la vulnerabilidad, todas apuntan a un riesgo central: afectar la integridad, disponibilidad y confiabilidad de la telemetría que alimenta al SIEM y a los sistemas de detección. Esto puede resultar en:

- ❑ Ceguera operativa ante movimientos laterales, intrusiones y actividad anómala.
- ❑ Manipulación de evidencia digital, elevando el riesgo reputacional y forense.
- ❑ Desvío de logs hacia servidores controlados por el atacante.
- ❑ Cargas falsas que saturan el monitoreo y retrasan la toma de decisiones.

COLCERT

Impacto para Colombia y la región

- **Sectores potencialmente expuestos:** financiero, gobierno, salud, TIC, energía, educación, transporte, comercio, industria y turismo.

- **Riesgo alto**: el riesgo es alto debido a la amplia adopción de Fluent Bit en infraestructuras críticas, entornos *cloud* y contenedores,especialmente en infraestructuras donde Fluent Bit se usa junto con Kubernetes, SIEM y observabilidad centralizada.. La explotación de estas fallas puede interrumpir la recolección de logs, alterar evidencia digital y comprometer la integridad del monitoreo, lo que incrementa la probabilidad de ataques dirigidos capaces de evadir detección en sectores estratégicos.

- **Posibles consecuencias**:
  - Pérdida parcial o total de visibilidad operativa en sistemas críticos.
  - Manipulación o desvío de *logs* que afecten investigaciones forenses y auditorías.
  - Interrupción de servicios esenciales debido a denegación de servicio en pipelines de monitoreo.
  - Ocultamiento de actividad maliciosa que facilite movimientos laterales, exfiltración o la ocultación de actividades asociadas a escalamiento de privilegios.
  - Incremento en tiempos de respuesta ante incidentes y aumento del impacto económico y reputacional.

- **Implicaciones en seguridad digital**: estas vulnerabilidades pueden comprometer la integridad, disponibilidad y confiabilidad de los sistemas de observabilidad y detección que soportan la ciberseguridad nacional y regional. La explotación podría permitir que actores maliciosos evadan controles, manipulen telemetría, degraden capacidades del Csirt y afecten la toma de decisiones estratégicas. Esto refuerza la necesidad de actualizar agentes, segmentar flujos de ingesta, endurecer configuraciones y monitorear anomalías en pipelines de logs en toda la región.

Técnicas MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Explotación de servicios remotos	T1210	Adversarios aprovechan vulnerabilidades en servicios expuestos para ejecutar código, inyectar datos o conseguir acceso no autorizado sobre el host que ejecuta Fluent Bit.
Explotación para escalamiento de privilegios	T1068	Uso de fallos de *software* para elevar privilegios en el sistema anfitrión, lo que permitiría a un atacante controlar más componentes.
Alteración de indicadores en el host	**T1070**	Técnicas para borrar o manipular artefactos y registros (logs). En este caso, la explotación de vulnerabilidades que permiten manipular tag_key o rutas de archivo facilita la supresión o alteración de evidencia en *pipelines* de *logging*.
Denegación de servicio en endpoints	T1499	Provoca la indisponibilidad de procesos o servicios locales, degradando la recolección de telemetría y la detección.

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Limitar el acceso a recursos por red	**M1035**	Restringir y segmentar el acceso a los endpoints de ingesta (HTTP, Forward, Splunk, Elasticsearch) reduce la exposición de *plugins* vulnerables y disminuye la probabilidad de explotación remota.
Gestión de cuentas privilegiadas	**M1026**	Asegurar que el agente se ejecute con cuentas de servicio con mínimos privilegios, rotación y control de credenciales limita el impacto de un RCE o escalamiento, evita que una explotación permita modificar amplias áreas del sistema o escribir archivos sensibles.
Restringir permisos de archivos y directorios	**M1022**	Evita que **Fluent Bit** (o procesos comprometidos) pueda escribir o reescribir artefactos críticos fuera de rutas previstas. Permisos estrictos sobre rutas de *logs* y archivos de configuración reducen la posibilidad de path traversal o sobreescritura de evidencia.
Prevención de ejecución	**M1038**	Controles de ejecución (*allow lists*, bloqueo de *scripts* no autorizados, control de carga de binarios) reducen la probabilidad de que código inyectado por una explotación se ejecute con éxito o que módulos no autorizados se carguen, mitigando impactos como RCE y reducción de disponibilidad.

Recomendaciones

- Actualizar la instalación de **Fluent Bit** a la versión más reciente disponible (≥ 4.2.0 / ≥ 3.0.4, según el caso), para asegurarse de incorporar los parches que corrigen las vulnerabilidades conocidas.
- Limitar el acceso de red a los "*input plugins*" expuestos (HTTP, Splunk, Elasticsearch, in_forward, in_docker, etc.), permitiendo únicamente fuentes confiables y redes internas, para reducir la superficie de ataque.
- Establecer rutas fijas y seguras para *outputs* de *logs* (definir explícitamente la opción *File* en configuraciones de salida cuando se use el *plugin file output*), evitando depender de etiquetas (tag_key) controlables externamente para determinar rutas de archivos.
- Ejecutar **Fluent Bit** con privilegios mínimos, correr el agente con un usuario no *root*, restringir permisos de escritura y lectura en directorios sensibles, y deshabilitar *plugins* innecesarios, para disminuir el impacto del potencial RCE o path traversal.
- Deshabilitar o aislar servicios de monitoreo o API de administración de **Fluent Bit** que no sean indispensables (por ejemplo, los endpoints internos de trazas), para reducir vectores de corrupción de memoria, DoS o divulgación de información.

Fuentes

CERT/CC (VU#761751), 24/11/2025, "Fluent Bit contains five vulnerabilities, including stack buffer overflow, authentication bypass, and path traversal", Advertencia de vulnerabilidad.
https://www.kb.cert.org/vuls/id/761751
INCIBE-CERT, 25/11/2025, "Múltiples vulnerabilidades en Fluent Bit", Aviso de seguridad.
https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-fluent-bit
NVD, 24/11/2025, 26/11/2025, "CVE-2025-12972 Detail – Fluent Bit out_file plugin does not properly sanitize tag values", Base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-12972
NVD, 24/11/2025, 26/11/2025, "CVE-2025-12970 Detail – Fluent Bit in_docker input plugin stack buffer overflow", Base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-12970
NVD, 24/11/2025, 26/11/2025, "CVE-2025-12969 Detail – Fluent Bit in_forward input plugin authentication bypass", Base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-12969
NVD, 24/11/2025, 26/11/2025, "CVE-2025-12977 Detail – Fluent Bit in_http/in_splunk/in_elasticsearch input plugins improper input validation of tag_key", Base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-12977
NVD, 24/11/2025, 26/11/2025, "CVE-2025-12978 Detail – Fluent Bit input plugins tag_key validation flaw", Base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-12978
Proyecto de desarrolladores (Fluent Bit), 12/11/2025, Fluent Bit release notes / announcement of patched version 4.2.0", Página oficial del proyecto.
https://github.com/fluent/fluent-bit/releases