Los investigadores de ciberseguridad han identificado cinco vulnerabilidades en Fluent Bit, un agente de telemetría ligero y de código abierto, que podrían encadenarse para comprometer y tomar el control de infraestructuras en la nube.

Los fallos de seguridad *«permiten a los atacantes evadir la autenticación, realizar recorridos de rutas, ejecutar código de forma remota, provocar condiciones de denegación de servicio y manipular etiquetas,»* señaló Oligo Security en un informe.

Una explotación exitosa de estas fallas podría permitir a los atacantes interrumpir servicios en la nube, alterar información y profundizar en las infraestructuras de nube y Kubernetes. Las vulnerabilidades detectadas son las siguientes:

CVE-2025-12972 – Una vulnerabilidad de recorrido de directorios causada por el uso de valores de etiquetas no sanitizados para generar nombres de archivos de salida, lo que hace posible escribir o sobrescribir archivos arbitrarios en el disco, permitiendo manipulación de registros y ejecución remota de código.
CVE-2025-12970 – Un desbordamiento de búfer en la pila dentro del plugin Docker Metrics (in_docker) que podría permitir a un atacante ejecutar código o provocar el fallo del agente creando contenedores con nombres excesivamente largos.
CVE-2025-12978 – Una falla en la lógica de coincidencia de etiquetas que permite a los atacantes falsificar etiquetas de confianza —asignadas a cada evento procesado por Fluent Bit— adivinando únicamente el primer carácter de un Tag_Key, lo que posibilita desviar registros, omitir filtros e inyectar datos maliciosos o engañosos bajo etiquetas confiables.
CVE-2025-12977 – Una validación incorrecta de datos de entrada en etiquetas derivadas de campos controlados por el usuario, lo que permite insertar saltos de línea, secuencias de recorrido y caracteres de control capaces de corromper registros posteriores.
CVE-2025-12969 – La ausencia de autenticación security.users en el plugin in_forward, utilizado para recibir logs de otras instancias de Fluent Bit mediante el protocolo Forward, lo que permite a un atacante enviar registros, introducir telemetría falsa y saturar los logs de un sistema de seguridad con eventos fraudulentos.

“El nivel de control que habilita esta clase de vulnerabilidades podría permitir a un atacante

penetrar más profundamente en un entorno en la nube para ejecutar código malicioso a través de Fluent Bit, al tiempo que decide qué eventos se registran, borra o reescribe entradas incriminatorias para ocultar su actividad, inyecta telemetría falsa e introduce eventos plausibles para confundir a los equipos de respuesta," indicaron los investigadores.

El CERT Coordination Center (CERT/CC), en un aviso independiente, afirmó que muchas de estas vulnerabilidades requieren que el atacante tenga acceso de red a una instancia de Fluent Bit, añadiendo que podrían utilizarse para eludir autenticación, ejecutar código de forma remota, causar interrupciones del servicio y manipular etiquetas.

Tras un proceso de divulgación responsable, los problemas fueron corregidos en las versiones 4.1.1 y 4.0.12 publicadas el mes pasado. Amazon Web Services (AWS), que también participó en la divulgación coordinada, instó a los clientes que utilizan Fluent Bit a actualizar a la versión más reciente para una protección óptima.

Dada la popularidad de Fluent Bit en entornos empresariales, estas deficiencias podrían afectar el acceso a servicios en la nube, permitir la alteración de datos y posibilitar que un atacante tome control del propio servicio de registro.

Entre otras acciones recomendadas se incluyen evitar el uso de etiquetas dinámicas para el enrutamiento, restringir rutas y destinos de salida para impedir expansiones o recorridos basados en etiquetas, montar *«/fluent-bit/etc/»* y los archivos de configuración como solo lectura para bloquear modificaciones en tiempo de ejecución, y ejecutar el servicio con usuarios sin privilegios de root.

Este desarrollo ocurre más de un año después de que Tenable detallara una vulnerabilidad en el servidor HTTP integrado de Fluent Bit (CVE-2024-4323, también conocida como *Linguistic Lumberjack*), que podía ser explotada para causar una denegación de servicio (DoS), divulgación de información o ejecución remota de código.