Google ha anunciado que su herramienta de fuzzing basada en inteligencia artificial, OSS-Fuzz, ha sido utilizada para identificar 26 vulnerabilidades en diversos repositorios de código abierto, incluyendo un defecto de gravedad media en la biblioteca criptográfica OpenSSL.

> *«Estas vulnerabilidades marcan un avance significativo en el uso automatizado para detectar fallos: cada una fue encontrada mediante IA, utilizando objetivos de fuzzing generados y mejorados con inteligencia artificial»*, explicó el equipo de seguridad de código abierto de Google en una entrada de blog.

La vulnerabilidad de OpenSSL en cuestión es CVE-2024-9143 (con una puntuación CVSS de 4.3), un error de escritura de memoria fuera de los límites que puede ocasionar una caída de la aplicación o la ejecución remota de código. Este problema ya ha sido solucionado en las versiones de OpenSSL 3.3.3, 3.2.4, 3.1.8, 3.0.16, 1.1.1zb y 1.0.2zl.

Google, que incorporó la capacidad de usar modelos de lenguaje grandes (LLM) para mejorar la cobertura de fuzzing en OSS-Fuzz en agosto de 2023, señaló que la vulnerabilidad probablemente ha estado presente en el código durante 20 años y que *«no habría sido detectada con los objetivos de fuzzing tradicionales creados por humanos.»*

Además, la compañía indicó que el uso de IA para generar objetivos de fuzzing ha incrementado la cobertura del código en 272 proyectos C/C++, añadiendo más de 370,000 líneas de código nuevo.

> *«Una de las razones por las que estos errores han permanecido ocultos por tanto tiempo es que la cobertura de líneas no asegura que una función esté libre de errores. La cobertura de código como métrica no puede medir todos los posibles caminos y estados del código; distintas configuraciones y opciones pueden provocar diferentes comportamientos, lo que puede desvelar distintos errores»*, señaló Google.

Estos hallazgos de vulnerabilidades asistidos por IA también son posibles porque los LLM han demostrado ser efectivos en emular el flujo de trabajo de fuzzing de un desarrollador, lo que facilita una mayor automatización.

Este avance ocurre después de que la empresa revelara a principios de mes que su sistema basado en LLM llamado Big Sleep ayudó a identificar una vulnerabilidad de día cero en el motor de base de datos de código abierto SQLite.

De forma paralela, Google ha estado trabajando para migrar sus propias bases de código a lenguajes más seguros en cuanto a manejo de memoria, como Rust, mientras implementa mecanismos para abordar vulnerabilidades espaciales en la memoria, que se presentan cuando un fragmento de código accede a memoria fuera de los límites definidos, en proyectos existentes en C++, como Chrome.

Esto incluye la transición hacia Safe Buffers y la implementación de libc++ reforzado, lo cual agrega verificaciones de límites a las estructuras de datos estándar de C++ para prevenir errores de seguridad relacionados con la memoria. También mencionó que el impacto en el rendimiento generado por estos cambios es mínimo (aproximadamente un 0.30% de impacto en el rendimiento).

> *«Libc++ reforzado, recientemente incorporado por contribuyentes de código abierto, introduce un conjunto de verificaciones de seguridad que ayudan a detectar vulnerabilidades como los accesos fuera de los límites en producción. Aunque C++ no se convertirá en un lenguaje completamente seguro en cuanto a memoria, estas mejoras reducen los riesgos [...], lo que resulta en un software más fiable y seguro»*, dijo Google.