La NSA finalmente lanzó el código fuente completo de GHIDRA versión 9.0.2, que ahora está disponible en su repositorio Github.

GHIDRA es la herramienta de ingeniería inversa de software clasificado localmente de la agencia que los expertos han utilizado internamente por más de diez años para detectar errores de seguridad en software y aplicaciones.

La herramienta está basada en Java, cuenta con una interfaz gráfica de usuario (GUI) y se ha diseñado para ser ejecutada en una variedad de plataformas que incluyen Windows, MacOS y Linux.

La ingeniería inversa de un programa o software implica el desensamblaje, es decir, la conversión de instrucciones binarias en código de ensamblaje cuando su código fuente no está disponible, lo que ayuda a los ingenieros de software, especialmente analistas de malware, a comprender la funcionalidad del código y la información de diseño e implementación real.

La existencia de GHIDRA fue revelada públicamente por primera vez por WikiLeaks, en las filtraciones de la CIA denominadas como Vault 7, pero hoy, la NSA lanzó públicamente la herramienta de forma gratuita en la conferencia RSA, lo que la convierte en una excelente alternativa a las costosas herramientas comerciales de ingeniería inversa como IDA-Pro.

> *«GHIDRA ayuda a analizar códigos maliciosos y malware como virus, y puede brindar a los profesionales de la ciberseguridad una mejor comprensión de las posibles vulnerabilidades en sus redes y sistemas»*, dice el sitio oficial de la NSA.

En los siguientes enlaces puedes descargar la herramienta y documentación:

- Github — Código fuente
- Download GHIDRA 9.0 — Paquete de software, diapositivas y ejercicios
- Installation Guide — Documentación básica

- Cheat Sheet — Atajos de teclado
- Issue Tracker — Reporte de errores

En la conferencia RSA, el asesor principal de la NSA, Robert Joyce, afirma que GHIDRA no tiene puerta trasera, y dice que *«Esta es la última comunidad a la que desea lanzar algo con una puerta trasera instalada, a las personas que buscan estas cosas para romperlas».*

Joyce también mencionó que GHIDRA incluye todas las características esperadas en las herramientas comerciales de gama alta, con una funcionalidad nueva y ampliada desarrollada de forma única por la NSA, y es compatible con una gran variedad de conjuntos de instrucciones de procesador, formato ejecutable y puede ejecutarse tanto en modo interactivo como automático.

> *«Módulos de procesador GHIDRA: X86 16/32/64, ARM / AARCH64, PowerPC 32/64, VLE, MIPS 16/32/64, micro, 68xxx, bytecode Java / DEX, PA-RISC, PIC 12/16/17 / 18/24, Sparc 32/64, CR16C, Z80, 6502, 8051, MSP430, AVR8, AVR32, otras variantes también»*, escribió en Twitter.

El primer bug reportado en la herramienta de ingeniería inversa GHIDRA

GHIDRA fue muy bien recibida por parte de la comunidad infosex, y los investigadores y desarrolladores comenzaron a contribuir al proyecto informando sobre errores y vulnerabilidades en Github.

Matthew Hickley, quien se hace llamar *HackerFantastic*, fue el primero en informar un problema de seguridad en GHIDRA. El error ya ha sido parchado en la última versión del software.

Hickey se dio cuenta de que la demanda de ingeniería inversa abre el puerto de depuración JDWP 18001 para todas las interfaces cuando un usuario inicia GHIDRA en el modo de

depuración, lo que permite que cualquier persona dentro de la red ejecute de forma remota un código arbitrario en el sistema de los analistas.

Aunque el modo de depuración no está activado de forma predeterminada y se supone que funciona de la manera prevista, el software debería escuchar solo las conexiones de depuración del host local, en lugar de cualquier máquina de la red.