Altra falla in Ghidra, il tool “open source” dell’NSA

Ott 01, 2019 Marco Schiaffino News, RSS, Scenario, Vulnerabilità 0

Il kit per il reverse engineering è stato messo a disposizione di tutti dalla National Security Agency lo scorso marzo. Ma a ogni bug c’è il sospetto…

Capita a tutti di incappare in qualche falla di sicurezza. Ci sono casi, però, in cui ogni bug che apre la strada a possibili attacchi solleva immediatamente polemiche e (soprattutto) sospetti.

Il caso di **Ghidra** ne è un perfetto esempio. Il tool dedicato al **reverse engineering** ha infatti il difetto di essere stato sviluppato da un soggetto che viene spesso guardato con sospetto da chi lavora nel settore della cyber-security.

Ghidra è infatti stato “regalato” da quella **National Security Agency** che, nell’immaginario collettivo, non rappresenta esattamente un modello di trasparenza e affidabilità. Insomma: ogni volta che spunta un bug in Ghidra, sul Web si diffonde il sospetto che la vulnerabilità sia stata inserita appositamente per consentire agli 007 di compromettere i PC su cui il software è installato.

La notizia, filtrata sabato scorso, riguarda una nuova vulnerabilità del software (CVE-2019-16941) che consentirebbe di portare attacchi in remoto per compromettere il sistema su cui gira Ghidra. **In pratica, il bug consentirebbe di avviare l’esecuzione di codice in remoto attraverso il caricamento di un documento XML**.



Come si legge nel report, l'attacco può essere portato solo se il software è impostato per utilizzare la "modalità sperimentale".

In questo caso, però, l'opinione di molti esperti è che il bug non sia poi così grave. Prima di tutto perché la modalità sperimentale, di per sé, suggerisce a partire dal nome il fatto che si tratti di una funzionalità che può avere qualche vulnerabilità.

C'è anche una discussione in corso riguardo l'effettiva possibilità di sfruttare la falla di sicurezza attraverso un attacco in remoto, ipotesi che alcuni ricercatori negano.

Tutta la vicenda, in ogni caso, conferma quanto la "operazione trasparenza" messa in atto dall'NSA stenti a dare frutti apprezzabili. Chi pensava che il rilascio di Ghidra potesse essere un modo per raffreddare i rapporti tra l'agenzia governativa e la community dei ricercatori, ha fatto male i conti.

Condividi l'articolo

Il settore energia è tra i più esposti alle minacce informatiche

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/10/01/altra-falla-in-ghidra-il-tool-open-source-dellnsa/