plugin_analyse_search_vulnerable_functions

Documentation

Description :

Plugin analysant les fonctions déassemblées pour trouver les instructions ASM inconnues.

- **Type :** PLUGIN_TYPE__ANALYSE
- **Priorité :** 50000
- **Nom du plugin :** plugin_analyse_search_vulnerable_functions

Fonctions recherchées :

- execle
- execvp
- execvpe
- getenv
- system

Infos nécessaires :

- Un gestionnaire de déassemblage doit avoir été choisi dans le champ « **ptr_func.deasm** ».
- Le binaire doit avoir été déassemblé.
- Les symboles correspondant aux adresses des fonctions vulnérables doivent être présent.

Effets :

- Une analyse « **Vulnerable functions** » est créée dans le champ « **analyses** ».
- Pour chaque fonction vulnérable à chercher, une sous-analyse ayant pour titre le nom de la fonction sera créée dans l'analyse « **Vulnerable functions »**.
- A chaque appel d'une fonction vulnérable, une sous-analyse ayant pour titre l'adresse de ce CALL sera créée dans la sous-analyse correspondant à la fonction recherchée.

Valeurs de retour :

- Retourne 1 si les appels de fonctions ont bien été analysés.
- Retourne 0 si le binaire n'a pas été préalablement déassemblé.
- Retourne -1 en cas d'erreur.