Rapport d'Analyse et de Détection des Vulnérabilités.

1. wolfSSH_SFTP_RecvWrite :

La faille que nous rencontrons est un **dépassement de tampon (buffer overflow)**. Un dépassement de tampon se produit lorsque le programme écrit plus de données dans un tampon (un espace mémoire alloué) que ce qui a été prévu.

Pourquoi cette faille se produit-elle ?

1. **Accès à la Mémoire :**
    - Dans notre cas, la fonction memcpy est utilisée pour copier des données dans une structure (probablement fd), mais la taille des données à copier (sz) n'est pas correctement vérifiée par rapport à la taille allouée pour fd. Si sz est supérieur à la taille de fd, cela écrasera la mémoire adjacente.
2. **Validation Insuffisante :**
    - Le code ne valide pas la taille des données avant de les copier. Si les données entrantes sont plus grandes que prévu, cela peut entraîner un dépassement.

2. wolfSSH_SFTP_RecvRead :

La faille que nous rencontrons ici est également un **dépassement de tampon (heap-buffer-overflow)**. Un dépassement de tampon se produit lorsque le programme écrit plus de données dans un tampon alloué sur le tas (heap) que ce qui a été prévu.

Pourquoi cette faille se produit-elle ?

1. **Allocation de Mémoire Insuffisante :**
    - Dans notre cas, la fonction WMALLOC est utilisée pour allouer de la mémoire pour out, mais la taille allouée peut être insuffisante pour contenir toutes les données qui y sont écrites. Si la taille calculée pour sz est incorrecte ou si des données supplémentaires sont ajoutées sans ajustement de la taille, cela peut entraîner un dépassement.
2. **Validation Insuffisante :**
    - Le code ne valide pas correctement la taille des données avant de les écrire dans le tampon. Si les données à écrire dépassent la taille allouée, cela écrasera la mémoire adjacente.

3. wolfSSH_SFTP_RecvRealPath:

La faille que nous rencontrons ici est également un **dépassement de tampon (stack-buffer-overflow)**. Un dépassement de tampon se produit lorsque le programme écrit plus de données dans un tampon alloué sur la pile (stack) que ce qui a été prévu.

Pourquoi cette faille se produit-elle ?

1. **Accès à la Mémoire :**
    - Dans notre cas, la fonction WMEMCPY est utilisée pour copier des données dans le tableau r, mais la taille de r n'est pas correctement vérifiée par rapport à la taille des données à copier (rSz). Si rSz est supérieur à la taille allouée pour r, cela écrasera la mémoire adjacente.
2. **Validation Insuffisante :**
    - Le code ne valide pas correctement la taille des données avant de les copier. Si rSz dépasse la taille de r, cela peut entraîner un dépassement.