Exploit d'accès au Kernel mode avec l'eLoader GTA sur 2.50 et 2.60 !

Soumis par SiZiOUS
28-06-2006

Un exploit a été trouvé par hitchhikr et Neural permettant à terme de lancer des programmes en kernel mode par la faille GTA sur le firmware 2.50 et 2.60. Il s'agit pour l'instant d'une Proof of Concept.

Marquez ce jour sur vos calendriers, car une petite révolution dans le monde de l'Homebrew sur PSP vient d'éclater. Un développeur connu sous le nom de hitchhikr de « hitchhikr SoftWorks » et son compagnon codeur Neural viennent de sortir la preuve d'un exploit sur les firmwares 2.5 et 2.6 !

Une fois implémenté et utilisé en mode « utilisateur normal », les firmwares 2.5 et 2.6 pourront béneficier des mêmes possibilités que le firmware 1.5 avec un accès COMPLET en mode kernel par l'intermédiaire du jeu Grand Theft Auto: Liberty City Stories comme avec l'eLoader.

Fanjita travaille déjà avec hitchhikr sur l'implémentation de ce nouvel exploit et également sur un moyen d'exécution facile via l'eLoader. Fanjita annonce déjà une application générique pour les développeurs dans les prochaines 24 heures. La sortie d'une application concrète pour les utilisateurs sera un peu longue ...

L'exploit tire profit de l'ajout de la fonction sceKernelLoadExec dans les firmwares 2.5/2.6 qui permet de lancement d'EBOOT, sensé être une sécurité supplémentaire ... Mais Sony a également accidentellement ajouté un bug d'overflow, ce qui signifie que l'exploit ne fonctionnera pas sur les firmwares 2.0 et 2.01.

Ci-dessous, vous trouverez le téléchargement de la preuve de l'exploit qui n'est pas destiné pour les simples utilisateurs comme nous. Il vous permet de dumper des fichiers contenu dans la mémoire kernel du firmware à la racine de votre Memory Stick (boot.bin, kmem.bin, klib.bin). Il crée également un fichier writeaccess.bin contenant le code hexadécimal (12 34 56 78), ce qui vous prouve que le kernel peut être écrit !

Mais ne commencez pas à upgrader vos PSP tant qu'il n'y aura pas un moyen viable d'exécuter des programmes via cette faille !

En outre, cette faille n'est pas un chemin vers un downgrader, du moins ce n'est pas une option envisageable au stade actuel de recherche. Bien que des spéculation ait déjà commencer en disant une éventuelle ouverture au décryptage du firmware 2.70+, et par la suite être émuler avec DevHook.

Cette faille n'ouvre absolument pas la voie vers un downgrade pour le moment à cause de la protection de l'IPL inclus dans les firmwares 2.50 et plus.

Traduction par crackjerem

Télécharger 2.5 and 2.6 Kernel Mode Unlocked Exploit

Source : benja32 sur le forum.

Site officiel : hitchhikr SoftWorks