Exploit Zelda Wii - lancer du code non signé sans puce

Soumis par redrum
27-01-2008

Oui, c'est celà. Un exploit pour la NIntendo Wii a été découvert et il permet de lancer du code custom. La méthode est assez simple. Copier une sauvegarde de Zelda , lancer le jeu et le code tourne. ne vous excitez pas trop encore. Ils n'ont été capables de faire tourner 4 lignes de code, mais après juste une journée de travail.

Segher a été celui qui a trouvé l'exploit et Bushing (le présentateur de l'exploit wii à la 24C3) l'a testé à l'aide du usb gecko. Le procédé est loin d'être
simple car il requiert la signature de la sauvegarde modifiée par 3 clés. Voilà quelques infos de Bushing.

"Quand la Wii décrypte la sauvegarde, elle vérifie sa signature. Chaque Wii a sa propre clé privée qui est utilisée pour signer les sauvegarde, et quand on sauvegarde, la Wii crée en fait 3 morceaux de données:

* la sauvegarde encryptée

* La signature pour la sauvegarde (utilisant la clé privée de la console)

* Une copie de la clé publique de la console, signée par NIntendo."

Bien sur, l'utilisateur final ne devrait pas avoir à refaire tout ce processus à moins de vouloir injecter son propre code dans la sauvegarde, mais celà ne devrait pas être nécessaire car quand interrogé sur le but final la réponse de Bushing a été:

"En présumant que ce ne soit pas une impasse, celà devrait permettre la création d'un lanceur de code homebrew (perso). J'espère. Pas de promesses :)"

Source - tehskeen