Wii Twilight Hack v0.1 Alpha1

Soumis par redrum
11-02-2008

La Team Twiizers (Segher, bushing, tmbinc) a publié son Twight Hack pour Nintendo Wii. Cet exploit permet de lancer du code custom en mode Wii. Cet exploit vient sous la forme d'une sauvegarde signée pour Zelda - The Twight Princess. Tout ce qu'il suffit de faire est copier la sauvegarde sur la wii via une carte SD, lancer le jeu, puis la sauvegarde...

L'info provient de wiibrew.org

[...]

Une fois chargée, allez parler à la personne la plus proche, ou marchez en arrière et le Beta Loader apparaitra avec un joli pinguin. Il détecte également si un SD Gecko ou USB Gecko est inséré. C'est donc tout pour l'instant, mais attendez-vous à une autre version bientôt qui vous permettra de lancer votre propre code.

Si vous êtes intéressé par des infos plus "poussées" vous devriez visiter wiibrew.org ;)

Tout celà a commencé quand les clés pour décrypter/encrypter les sauvegardes furent trouvées. Une fois celà fait, les auteurs (Segher, Bushing et Tmbinc) ont pu commencer à jouer avec les données de sauvegarde. Celà a mené à un bug dans le jeu Zelda, qui permettait de "crasher" le jeu..

Une fois dans cet état, il leur fut possible de lancer quelques bytes de
code. Après celà ils réussirent à augmenter la taille du code - assez pour créer une démo qui est cet exploit.

Dû au fait qu'ils savent comment encrypter les données de sauvegarde et les signer, celà permet à n'importe quel utilisateur de lancer cet exploit sans que celà requiert la moindre intervention sur la machine (pose de puce, etc.)

L'exploit actuel peut détecter la présence d'un SD Gecko ou USB Gecko. Si vous avez un USB Gecko connecté, il lui enverra un peu de texte mais c'est tout.

Ci-dessous une vidéo de l'exploit: de la copie de la sauvegarde hackée jusqu'à son lancement

Segher a déclaré qu'ils travaillent sur une nouvelle version et que quelques unes des fonctions en préparation sont le chargement de code depuis un SD Gecko/ USB Gecko, mais le moyen principal de lancer du code et sur lequel ils se concentrent est soit par USB et Wi-Fi ou bien simplement depuis le port SD intégré à la Wii.

C'est un grand moment dans la scène homebrew wii. Bientôt nous pourrons lancer du code homebrew grâce à Segher, Bushing et Tmbinc.

Télécharger twilight-hack-v0.1-alpha1.zip

Source tehskeen.com

Note: Si vous voulez plus d'infos, une interview de Bushing a été réalisé le 28 Janvier par le site atomicmpc.com (en anglais)

Voir ici: http://www.atomicmpc.com.au/article.asp?SCID=14&CIID=102079