Sécurité des ordivisions

SSTIC 2014
Frédéric Basse

Qu’est-ce-qu’un ordivision ?

Agenda

- Cible & Objectifs
- Présentation
- Exploitation
- Exploration
- Persistance
- Conclusion

Cible & Objectifs

- SmartTV grand public
  - **1 constructeur**
  - **2 modèles étudiés : 2011 & 2013**
    - Architecture matérielle identique
    - Une architecture alternative existe (basée ARM).
- Aperçu de la sécurité
  - **Boîte noire**
  - **Connectée**
- Fun

Présentation

Fonctions des SmartTV

- **Applications connectées**
  - **Navigateur Web**
  - **Email**
  - **Apps: Skype, Facebook, …**
  - **Streaming VOD**
  - **Cloud TV (-_-)**
  - **Cloud Explorer (-_-')**
- **Accès aux contenus multimédia du LAN**
- **Techno Miracast : partage d'écran**
- **Mises à jour système par Internet**

Architecture

- OS Linux
- Processeur MIPS32
- Mémoire flash : système & settings
- Ethernet
- AP Wifi : Miracast
- USB
- UART
- Télécommande infrarouge / ZigBee

Collecte d'informations

- Code sources sous licences libres : U-Boot, noyau Linux, patchs, …
  - **Indiquent la présence de mécanismes Secure Boot**
- UART : prise jack 3.5 sur le panneau arrière
  - **Sortie console U-Boot / Kernel**
  - **Informations techniques pertinentes**
    - Informations sur l'activité des processus
    - Détails des crashs éventuels
- Scan réseau
  - **Service UPnP: libupnp 1.4 d'après l'entête**

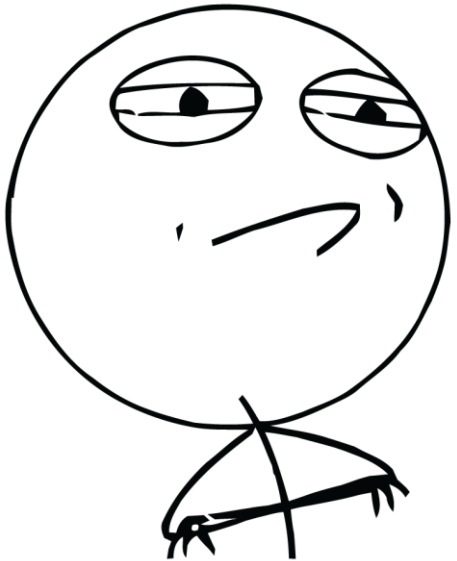
Exploitation (1/2)

Vulnérabilité libupnp : CVE-2012-5958

- ***Remote stack overflow*** **découvert par Rapid7 fin 2012**
- **Un simple paquet UPnP (UDP) pour déclencher le bug**
  - Erreur générée sur la sortie console :

    SIGSEGV: address not mapped to object:

    process = dlnaApp (677), epc = 0x41414141, ra = 0x0049ec8c
  - Absence de *Stack-Smashing Protector*
- **Non-corrigé sur firmware de 2014**
- **Exploitation pas évidente**
  - Binaire non accessible, projection en mémoire inconnue



Exploitation (2/2)

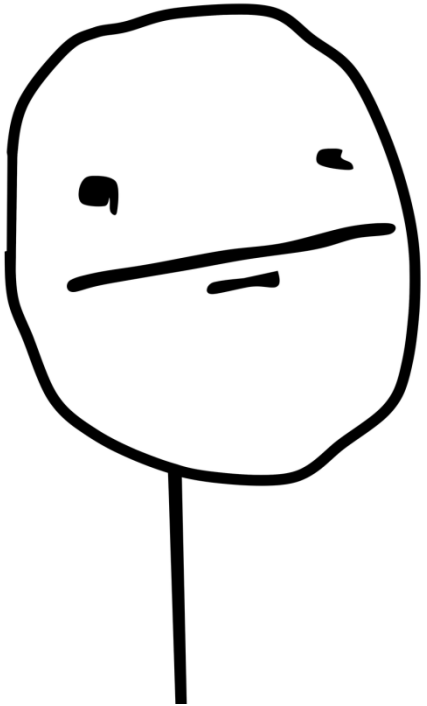
Technique d'exploitation CVE-2012-5958

- **Cross-compilation de libupnp avec des conditions similaires à la cible**
  - Version, architecture, compilateur
- **Analyse du binaire libupnp factice**
  - Des registres sauvegardés sur la pile peuvent être réécrits
- **Déduction de la projection en mémoire du binaire cible**
  - Observation des effets de l'altération de ces registres
- **Injection, localisation et exécution du shellcode dans le tas**
  - Recherche de string à une adresse arbitraire
- ***Détails dans les actes***

Exploration (1/3)

Processus

- **Permissions root (tous)**
- **Pile et tas exécutables**
- **Tas non-randomisé**
  - Pas supporté dans cette version du noyau Linux
- ***Stack-Smashing Protector* parfois, selon les binaires**



Exploration (2/3)

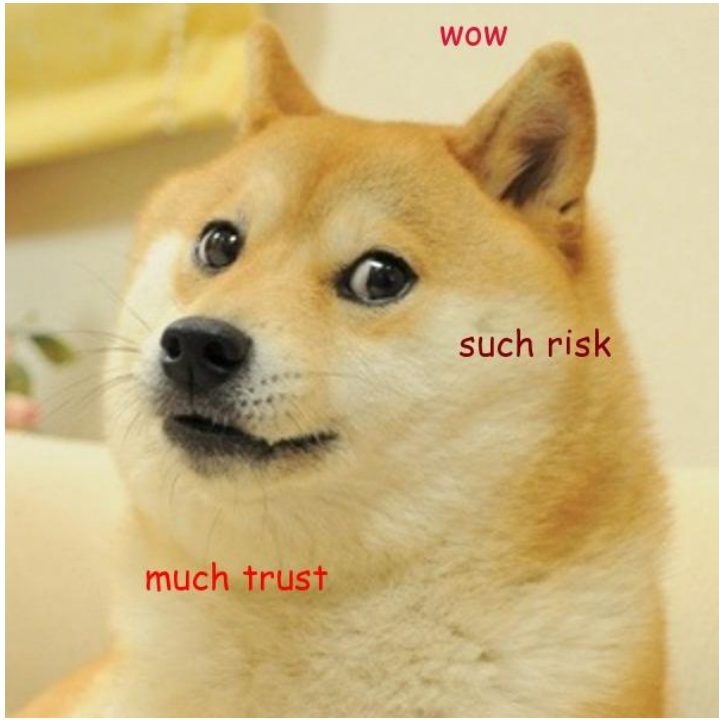
- Fichier de mise à jour
  - **Téléchargeable sur le site Web du constructeur**
  - **Signé RSA 1024 : clé publique différente pour chaque modèle de TV**
  - **Chiffré AES 256 : clé dans la signature**
  - **Contenu : image système, script de mise à jour, settings par défaut, …**
- Programme de mise à jour
  - **Aucune vulnérabilité découverte**
- Outil d'extraction des mises à jour
  - **github.com/frederic/pflupg-tool**

Exploration (3/3)

- DirectFB : alternative au serveur X Window
  - **Gestion de l'accélération graphique matérielle, périphériques d'entrées et des fenêtres au travers de l'interface framebuffer de Linux**
- Voodoo : couche réseau (« proxy ») pour des applications DirectFB distantes
  - **Port TCP ouvert sans filtrage ni authentification**
  - **CVE-2014-2977 integer signedness vulnerability**
  - **CVE-2014-2978 remote out-of-bounds write vulnerability**
- Dissecteur Wireshark pour le protocole Voodoo de DirectFB
  - **github.com/frederic/dfb-wireshark-dissector**

Persistance

- Vecteur de persistance
  - **Partition système SquashFS: lecture seule**
    - Signée avec RSA
  - **Partition données UBIFS: lecture & écriture**
    - Fichiers de configuration, aucun binaire/script
- Actions au démarrage
  - **Lecture d'un fichier de la partition données**
    - fscanf(file,"%s", buffer_on_stack)
  - **Débordement de mémoire => Persistance**
  - **Persiste après mise à jour du firmware**



Conclusion

- **Beaucoup d'efforts pour préserver l'intégrité du système**
  - Secure Boot
  - Mises à jour chiffrées, signées
- **Moins pour protéger les utilisateurs**
  - Peu de mécanismes de protection contre l'exploitation logicielle
  - Vulnérabilités publiques non-corrigées
  - Données de l'utilisateur non-chiffrées
- **Ne pas connecter à un réseau sensible, dans un lieu sensible**

Questions ?

- **Contact : fredericDOTbasseATthalesgroupDOTcom**