Demonstration

# Requirements

* Operating System: Windows 7 Professional x64 SP1, updated up to April 1st (iso: en\_windows\_7\_professional\_with\_sp1\_x64\_dvd\_u\_676939.iso)
* CPU: Intel Nehalem or Sandy bridge micro-architectures. Tested on:
  + Intel Xeon E5620
  + Intel i7 2600S

# Disable driver signature enforcement

Press F8 while booting into Windows and select “Disable Driver Signature Enforcement” in Advanced Boot Options – shown in Figure 1. If this is not set, kBouncer will not be able to load the driver, as it is not signed.

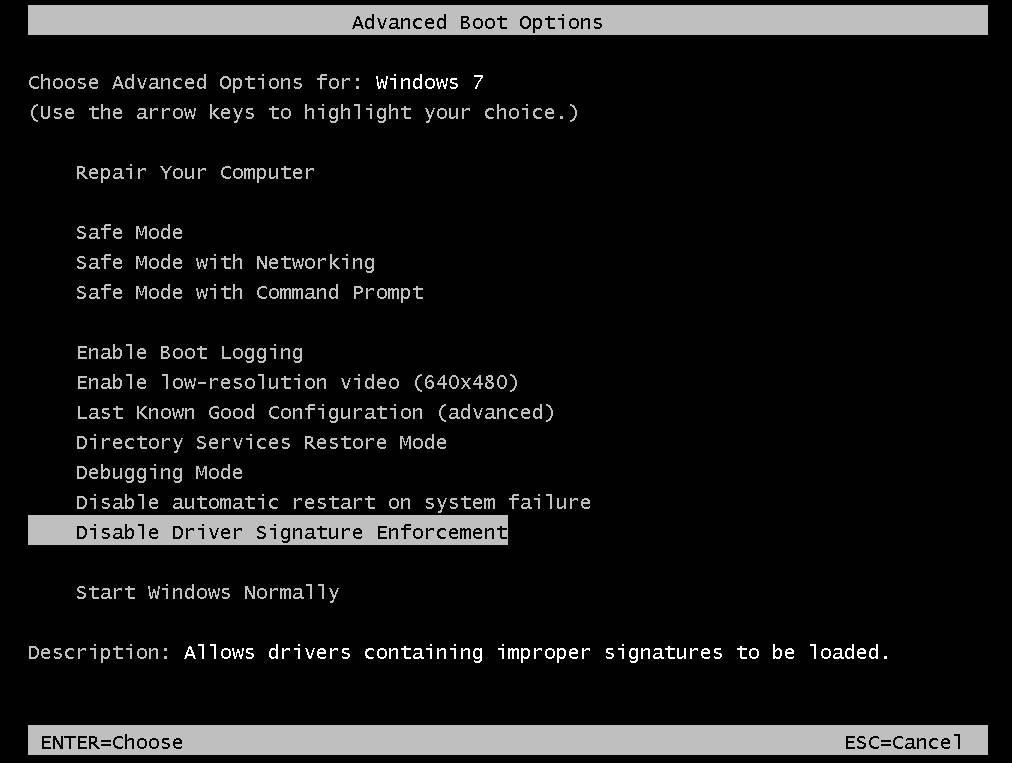


Figure . Advanced Boot Options: Disable Driver Signature Enforcement

# Start a cmd.exe as administrator

Press Start menu, search for cmd, right-click on the result and select “Run as administrator” (Figure 2). Then change to the directory that kBouncer was extracted (preferably C:\kbouncer).

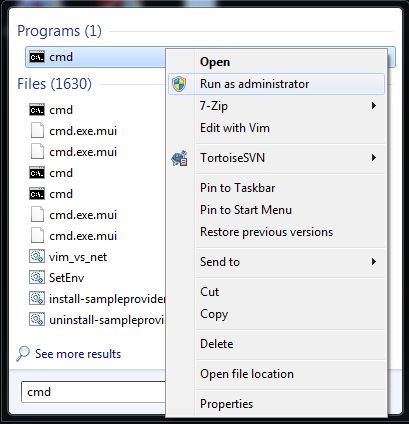


Figure . Run cmd.exe as administrator

# Test that the driver is working

* Load the driver by executing “**start run.bat**” in the bin directory of kBouncer. A new cmd.exe window will open and inform you whether the loading was successful or not. Do not press any key in that window, as it will unload the driver. Ignore any warning pop ups about driver’s signature (Figure 3). This window must remain open during the demonstration!
* Execute the **test.exe** program in the bin directory of kBcouncer. This program checks whether the CPU supports the LBR feature, performs an abnormal return control transfer (check src/windows/drv/exe/test.c) and then asks the driver component to check the LBR. So, an alert like the one in Figure 4 should pop up if everything is working correctly. If not, then something is wrong. Maybe driver signature enforcement was not disabled, or the CPU does not support the LBR feature (check the console output of test.exe). Please contact me if the problem insists and I can check if there is any other incompatibility. Use this window to issue any commands you are asked from now on.

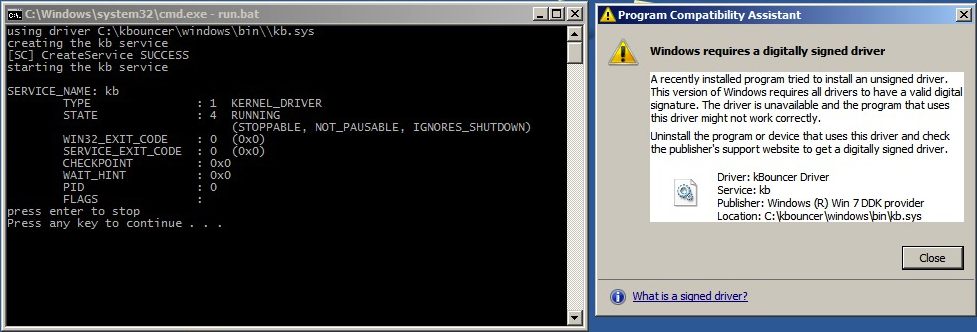


Figure . Load the driver and ignore the warning.

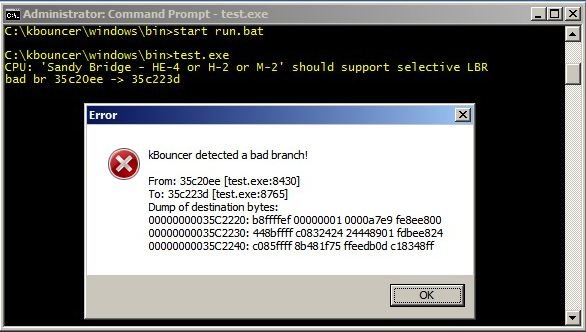


Figure . If the driver works correctly you should see an alert like this.

# Adobe Reader Exploit

## Check that the exploit works

* Download Adobe Reader v9.3.4 from here: <http://www.oldapps.com/adobe_reader.php?old_adobe=24>
* Install it and do not update it!
* Start Reader, click File -> Open, navigate to the bin directory of kBouncer and select the CVE-2010-2883…pdf file. This file was constructed using the metasploit script from: <http://www.exploit-db.com/exploits/16619/>
* Close any crash dialog that may appear and click on Open. Adobe Reader installs a shell extension that usually crashes when you select the pdf file in the open file dialog, but that does not affect the exploit when the file is opened.
* After clicking Open, the exploit in the pdf file should replace Adobe Reader with the Calculator applications (the exploit calls WinExec(“calc.exe”)).

## Check that kBouncer can prevent the exploit

Switch to the cmd.exe window and execute:

**withdll.exe /d:kb.dll “C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd32.exe”**

The second argument is the file path to the Reader executable. If it is install in another directory, use the appropriate one.

Then, open the exploit file again. This time an alert window from kBouncer should appear before Calculator is started! (Figure 5)

In rare cases, mostly on Nehalem, kBoucner was not able to prevent the exploit the first time on a fresh install of Reader. I didn’t have enough time to investigate this bug, so if it occurs, please try again or try the MPlayer first or reboot ☺

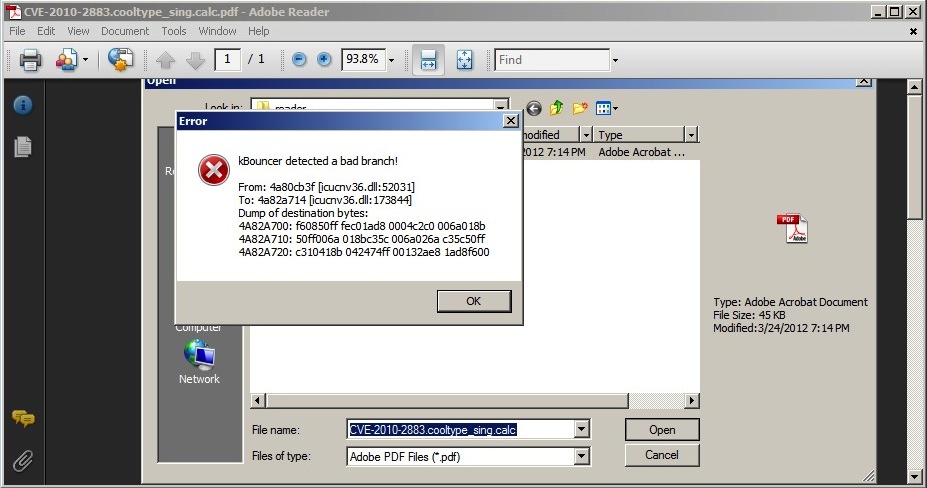


Figure . kBouncer preventing the Adobe Reader exploit!

# MPlayer Exploit

## Check that the exploit works

* Download the vulnerable version (MPlayer Lite r33064) from here: <http://www.exploit-db.com/wp-content/themes/exploit/applications/aa7e6d4ad9054e26df931bd5bda1e636-mplayer_lite_r33064.7z>
* Extract it (you may need 7z from <http://www.7-zip.org/>). You do not need to execute any install script. Simply double-clicking the mplayer.exe executable can start MPlayer.
* As you can see there are a few .m3u files in the bin directory of kBouncer. The reason for that is because this exploit was originally for an older version of kernel32.dll (6.1.7601.17514) and we had to manually update it to work with the latest (6.1.7601.17651) because the offset of the VirtualProtect function was changed. Also, for some reason, the stack frame is shifted by a few hundreds of bytes when Windows are running on the i7 CPU instead of a Core 2 or Xeon. That is why there are two versions of the newer exploit.
* Start mplayer.exe, click the upper left corner, select File -> Open, navigate to the bin directory of kBouncer, select mplayer.win7sp1.calc.6.1.7601.17651-i7.m3u and click Open. If the exploit works, it should replace the MPlayer application with the Calculator (same shellcode as in the Adobe Reader’s).
* If it doesn’t work, try to open the other .m3u files. More precisely, mplayer.win7sp1.calc.6.1.7601.17651-i7.m3u should work on Sandy Bridge processors and mplayer.win7sp1.calc.6.1.7601.17651.m3u on Nehalem ones.
* If none works, please let me know. It was a little bit hard getting this exploit to work. The original exploit was constructed using the script from: <http://www.exploit-db.com/exploits/17124/>.

## Check that kBouncer can prevent the exploit

Switch to the cmd.exe again and execute:

**withdll.exe /d:kb.dll “C:\Users\vpappas\Desktop\mplayer\mplayer.exe”**

Again, the second argument is the location of the MPlayer’s executable and should be the location where MPlayer was extracted.

Then, open the exploit file again. This time an alert window from kBouncer should appear before Calculator is started! (Figure 6)

Most of the times, the alert window appears behind the MPlayer’s window, so after opening the exploit file, check (using Alt-Tab) if a new window was opened!

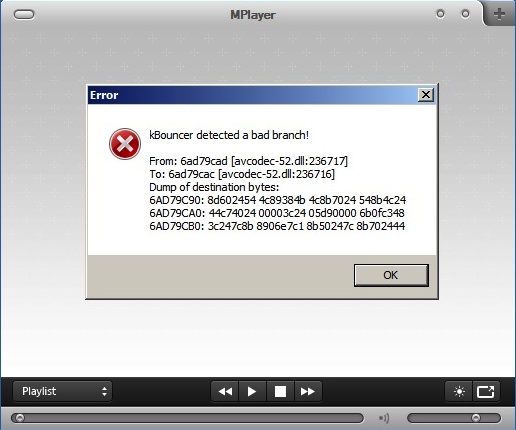


Figure . kBouncer preventing the MPlayer exploit!

I hope it worked! Thanks for your time!