

# Forum:[Hack Forums](#)

Thread: [Windows 7 authentication Bypass](#)

**mudasir007** - October 15, 2014, 8:10 am

## Windows 7 Zero Day Authentication Bypass Exploit

The Credit for this Exploit goes to nooby\_at\_safengine.com. It is still a Zero day exploit i think Microsoft didn't released any patch for it. It allows guest users to bypass windows authentication and acquire system privileges. The prerequisites for this exploit are default installation of windows 7 and guest account on windows also please shutdown the malwarebytes while you play with the exploit

### How to Exploit

The Exploit Comes with (Proof of the concept) POC.Exe. Simply you have to run poc.exe in cmd shell it also come with a video you can play it in Browser

1. Create a Guest account in windows 7
2. Open Cmd and type whoami You will get response user/guest
3. Place the Exploit ie POC.exe in your C:\ Drive or in any folder like Public folder
4. open up CMD and type Cd C:\ . You Will get C:\> Prompt in cmd shell
5. Now in CMD type poc and enter you will again get C:\> prompt
6. Now type whoami and you will get NT User /System.
7. Oh my God You Have acquired System from Guest account and simply type net user hacker 007 and net user hacker administrator and you have created administrator account on system

### How it works

According to website Exploit db the registry value which will precisely overwrite the return address of the calling function on stack, results in an arbitrary buffer being executed in kernel mode. In PoC the buffer contains a simple kernel PE loader, which will eventually load a driver that will escalate "cmd.exe" process privilege regardless of UAC.

### The Kernels it Supports

Windows Vista/2008 6.1.6000 x32,  
Windows Vista/2008 6.1.6001 x32,  
Windows 7 6.2.7600 x32,  
Windows 7/2008 R2 6.2.7600 x64

### Conclusion

Released in November 2010 still a zero day all praise goes to Exploit coder and has helped me Escalate from guest to admin it is just awesome The exploit comes with a video watch it also the Exploit can be downloaded at address <http://www.exploit-db.com/splotts/uacpoc.zip> Please report back and say thanks

Note This Exploit will only work when AV is temporary shutdown otherwise it wont work once the av gets its signature

please don't do any illegal activity i am not responsible??

**Faded™** - October 15, 2014, 9:19 pm

this bypasses the activation prompt? after the 30 days?

**mudasir007** - *October 16, 2014, 5:53 am*

(Oct 15, 2014 09:19 PM)Faded™ Wrote: [\[CITE\]](#) this bypasses the activation prompt? after the 30 days?this is authentication bypass and you don't have to provide Administrator password as you get system shell where you get kernel privileges