

Security vulnerability discovered on Windows 7, affecting millions of users

A security hole has just been discovered in Windows 7 that can affect millions of users. Security researchers recently found a local privilege vulnerability in Windows 7 that could affect millions of Windows users who haven't updated since this release.

Discovered in November, this vulnerability also exists in Windows Server 2008 R2 and Windows 10. Devices running either version of Windows are vulnerable.

According to security researchers, an exploited vulnerability can be extremely serious. While it is not as vulnerable to exploitation as other vulnerabilities found in the system, with an understanding of Windows 7, an attacker can alter the Performance Monitoring System with the privileges that the vulnerability provides. allows the attacker to execute any selected code.

```

Y:\6867_2P-516_advap132\4E61200124545_64bit\pp - Notepad
File Edit Format View Help
MODULE_PATH ..\Affected_Modules\advap132.dll_6.1.7601.24545_64bit\advap132.dll
PATCH_ID 516
PATCH_FORMAT_VER 2
VULN_ID 6867
PLATFORM win64

patchlet_start
PATCHLET_ID 1
PATCHLET_TYPE 2
PATCHLET_OFFSET 0x166fac
N_ORIGINALBYTES 5
JUMPOVERBYTES 0
PIT revert!strncmp,advap132!0x170aa

code_start
mov cx, word[rip+0Ch] ; [rip+0Ch] current registry/service name length
cmp cx, 18h ; 18h widechar length of RcpptMapper
jz ERCEPTIONMAPPER ; if length of current registry/service is the same compare strings

cmp cx, 10h ; 10h widechar length of Descache
jnz CONTINUE ; if length of current registry/service not the same continue execution

call VAR ; push WR1 to stack
dw __utf16__('Descache') ; registry/service to avoid from being processed

VAR:
pop rcx ; rcx = widechar Descache (string1)
lea rdx, [rip+10h] ; [rip+10h] current registry/service name(widechar, string2)
mov r8, 10h ; size to compare
call PIT_strncmp ; compare string1 and string2
cmp eax, 0 ; if eax = 0 then the strings are identical
jnz CONTINUE ; if eax < 0 then continue with execution
jmp EXITLOOP ; eax = 0

ERCEPTIONMAPPER:
call VAR2 ; push WR2 to stack
dw __utf16__('RcpptMapper') ; registry/service to avoid from being processed

VAR2:
pop rcx ; rcx = widechar RcpptMapper (string1)
lea rdx, [rip+10h] ; [rip+10h] current registry/service name(widechar, string2)
mov r8, 10h ; size to compare
call PIT_strncmp ; compare string1 and string2
cmp eax, 0 ; if eax = 0 then the strings are identical
jnz CONTINUE ; if eax < 0 then continue with execution

EXITLOOP:
jmp PIT_0x170aa ; jump to end of loop

CONTINUE:
; continue normally
code_end

patchlet_end
    
```

A critical security hole that exists on Windows 7 has just been discovered

In a nutshell, this security vulnerability can affect the user's privacy and resources to the fullest extent when fully exploited, with write access to the following registry keys:

HKLM SYSTEM CurrentControlSet Services Dnscache

HKLM SYSTEM CurrentControlSet Services RpcEptMapper

The bigger problem is that the Microsoft team won't do much to help endangered users. Since Microsoft has moved into the era of Windows 10 and its updates, Windows 7 users will not see any solutions made by Microsoft to this important issue. This has left millions of people dependent on third-party solutions or complete upgrades from the OS.

Fortunately, a cybersecurity company called 0patch has helped users get rid of the dangers of this vulnerability. Users using the affected versions can download it for free at [here](#) .

You finished reading the article "**Security vulnerability discovered on Windows 7, affecting millions of users**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.