# 48Bits Advisory: Path conversion design flaw in NTDLL -=- www.48bits.com

There is a design flaw in the way that NTDLL performs path conversion between DOS style path names and NT syle path names. Although many attack vectors are possible, in this paper some proof of concept cases are covered.

## Vulnerability details:

The vulnerability is located in the exported function RtlDosPathNameToNtPathName_U which converts from unicode DOS path names to unicode NT path names.

RtlDosPathNameToNtPathName_U internally checks if the given path name is already in NT style or is in DOS style, calling respectively RtlpWin32NTNameToNtPathName_U or RtlGetFullPathName_Ustr. Is in these functions where each proper syntax (NT and DOS styles) are checked.

When a given path name ends with one or more space characters, RtlpWin32NTNameToNtPathName_U keeps them in the returned path, RtlGetFullPathName_Ustr instead, removes them, here is where the design flaw comes into play, because space finished DOS style paths given won´t return the real NT style path when indeed is possible to create such NT style file names.

## Affected software:

Any program that relies on RtlDosPathNameToNtPathName_U the conversion between DOS paths to NT paths, are prone to unproperly handle such files. The following Operating System files import and use the function:

```
acledit.dll
ADVAPI32.DLL
cscdll.dll
CSRSRV.DLL
dskquoui.dll
EVENTLOG.DLL
GDI32.DLL
ifsutil.dll
KERNEL32.DLL
LSASRV.DLL
ntmarta.dll
OLE32.DLL
perfproc.dll
query.dll
rshx32.dll
scesrv.dll
sdbapiu.dll
setupdll.dll
sfc.dll
SHELL32.DLL
shim.dll
srvsvc.dll
trkwks.dll
ulib.dll
wow32.dll
AUTOCHK.EXE
autoconv.exe
autofmt.exe
NTVDM.EXE
os2srv.exe
posix.exe
regsvc.exe
SERVICES.EXE
smss.exe
WINLOGON.EXE
```

Usually, third party applications for Windows environment, use KERNEL32.DLL or intermediate Dynamic Link Libraries,like MSVCRT.DLL, for file managing tasks.

The following KERNEL32.DLL functions make use of RtlDosPathNameToNtPathName_U:

GetShortPathNameW
CopyFileW
MoveFileW
MoveFileExW
ReplaceFileW
CreateMailslotW
GetFileAttributesW
FindFirstFileExW
CreateFileW
GetVolumeInformationW
DeleteFileW
GetDriveTypeW
GetFileAttributesExW
CreateDirectoryW
FindFirstChangeNotificationW
GetBinaryTypeW
CreateNamedPipeW
SetFileAttributesW
MoveFileWithProgressW
GetVolumeNameForVolumeMountPointW
GetDiskFreeSpaceW
CreateDirectoryExW
DefineDosDeviceW
PrivMoveFileIdentityW
GetCompressedFileSizeW
SetVolumeLabelW
CreateHardLinkW
RemoveDirectoryW

As we can see there are involved lot of important functions, which are used for tasks like create a new file, delete a file, etc ... although the vulnerability is located in ntdll, third party applications are affected as well as Windows applications like explorer.

Attack Vectors:
---------------

As well as there can be many vector attacks, some perhaps more dangerous, i have successfully exploited two of them:

- Not accessible or erasable file:

A file with a name like:

NT Filename: "\\?\C:\test "

Wont be accessed or erased by calling KERNEL32.DLL APIs giving the DOS path name:

DOS FIlename: "C:\test "

- Redirecting files:

Suppose we have a file like this

NT FileName:  "\\?\C:\test"

And in the same directory another file like this:

NT FileName: "\\?\C:\test "

All operations performed by vulnerable APIs to the DOS path name:

DOS FileName: "C:\test "

Will be done to the first file.

## Affected Platforms

Tested on W2kSP4 and WXPSP2 but others might be vulnerable.

## Real life affected software:

The attack vectors explained before, usually don´t pose a threat for the end user, one exception is security software, and more precisely antivirus and antispyware software. I have tested the not accessible or erasable proof of concept file, containing inside malware testing signatures, with the latest versions of some of them and here are the results:

Vulnerable antivirus:

* BitDefender:
  - Resident shield unable to detect and disinfect
  - On demand unable to detect and disinfect.

* Norman:
  - Resident shield unable to detect and disinfect.
  - On demand unable to detect and disinfect.

* Norton antivirus (2006):

  - Resident shield able to detect, unable to desinfect.
  - On demand unable to detect and disinfect.

* Antivir XP:
  - Resident shield able to detect (but doesn´t show an alert), unable to desinfect.
  - On demand unable to detect and disinfect.

* F-Prot:

  - Resident shield able to detect but unable to disinfect
  - On demand unable to detect and disinfect.

* Nod32:

  - Resident shield able to detect but unable to disinfect
  - On demand unable to detect and disinfect

* AVG:

  - Resident shield able to detect but unable to disinfect
  - On demand unable to detect and disinfect.

* Avast:

  - Resident shield able to detect but unable to disinfect
  - On demand unable to detect and disinfect.

* Kaspersky (Personal 5):
  - Resident shield able to detect and disinfect
  - On demand unable to detect and disinfect

Vulnerable AntiSpyware:

* SpySweeper:

  - Unable to detect and disinfect.

* Spybot search and destroy:

  - Unable to detect and disinfect.

* Ad-Aware:

  - Unable to detect and disinfect.

Not Vulnerable:

* Panda (Tested IS 2006)<br>
* Macaffe

Proof of concept:
-----------------

There is no need for complex code here ;-), just take a look at what happens when you type the following in a cmd.exe:

```
echo X5O!P%@AP[4\PZX54(P^^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*>"\\?\C:\malware.exe "
```

and play around this file :-)

Vulnerability discovered and analysis Performed by:
---------------------------------------------------

Mario Ballano Bárcena  mballano[4t]gmail.com

[48Bits I+D team] -=-  www.48bits.com

-= EOF =-