New Attack Vectors
and a
Vulnerability Dissection
of
MS03-007

An NGSSoftware Insight Security Research publication
21st March 2003

David Litchfield
(david@ngssoftware.com)

www.ngssoftware.com

Introduction

The patch announced by Microsoft on the 17th March 2003 fixed a security vulnerability in the core of the Windows 2000 operating system. This flaw was actively being exploited through WebDAV requests to Microsoft's Internet Information Server 5. It must be stressed that IIS was simply the attack vector; the method or route used to actually exploit the flaw. The problem, however, is much wider in scope than just simply machines running IIS. Researchers at NGSSoftware have isolated many more attack vectors including java based web servers and other non-WebDAV related issues in IIS. Due to this, NGSSoftware urge Windows 2000 users to apply the patch.

Vulnerability Dissection
As far as the IIS vector is concerned WebDAV requests do not limit the length of the file name being requested. When processing a WebDAV based request, whether the method used is PROPFIND, LOCK, SEARCH or even GET with the "Translate: f" header, the request is passed through a series of functions, one of these being GetFileAttributesExW. Under the hood of GetFileAttributesExW is a call to the RtlDosPathNameToNtPathName_U function exported by ntdll.dll. This is where the actual vulnerability lies.

RtlDosPathNameToNtPathName_U relies on unsigned shorts for string lengths. As unsigned shorts are 16 bits in size they can hold a number from 0 to 65535. If a string is 65536 bytes long then the length of the string is considered as being 1 byte long - whereas in actual fact the string is considerably longer. Due to this reliance on unsigned shorts the vulnerability exists.

GetFileAttributesExW is not the only function that calls RtlDosPathNameToNtPathName_U. There are many:

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 can be seen most of these functions deal with the file system, and for a piece of software to be a "suitable" attack vector an attacker must be able to supply an arbitraryily long string to any one of these functions. But then other functions in different DLL's also rely on RtlDosPathNameToNtPathName_U. These are some of the other DLLs that import this function

acledit.dll
advapi32.dll
cscdll.dll
csrsrv.dll
dskquoui.dll
eventlog.dll
gdi32.dll
ifsutil.dll
lsasrv.dll
ntdll.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
svcpack.dll
trkwks.dll
ulib.dll
wow32.dll

Conclusion
Security researchers at NGSSoftware have already discovered several new attack vectors and believe there will be many that will come to light over the next few weeks. There are too many

ways for an attacker to "access" the vulnerability. Likely areas will be Non-MS web and ftp servers, IMAP servers, Anti-Virus solutions and other MS Windows Services.

Consequently, NGSSoftware believes that every Windows 2000 server or workstation should be patched, and patched as soon as possible – regardless of whether the box is running IIS or not.

Resources
Microsoft Advisory:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-007.asp
Patch (All except Japanese NEC):
http://microsoft.com/downloads/details.aspx?FamilyId=C9A38D45-5145-4844-B62E-C69D32AC929B&displaylang=en
Patch (Japanese NEC):
http://microsoft.com/downloads/details.aspx?FamilyId=FBCF9847-D3D6-4493-8DCF-9BA29263C49F&displaylang=ja