IOActive Security Advisory

Title	Windows Kernel Library Filename Parsing Vulnerability
Severity	Critical
Discovered by	Lucas Apa
Microsoft Security Bulletin	December 2012
Bulletin ID	MS12-081
CVE	CVE-2012-4774
Disclosure	Coordinated with Microsoft

Technical Details

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Windows. User interaction is required to exploit this vulnerability in that the target must open or browse to a file or subfolder with a specially crafted name on a network SMB share, a UNC share, a WebDAV web folder. Other specific file system drivers could trigger the vulnerability remotely if resources are accessible over a storage area network where all nodes directly access the block storage where the file system is located. In a web attack scenario, an attacker would have to host a website that contains a file with a specially crafted name since some browsers redirect URI's to the explorer.exe process.

The vulnerability exists in a critical operating system DLL, so it could be exploited when a user land application browses the file system using the Windows API, such as when opening a folder (File->Open). This scenario allows more specific exploits to be created for each application which uses the aforementioned DLL.

Routines within the KERNEL32.DLL dynamic link library do not properly validate substructure elements before using them to manipulate memory. This can lead to memory corruption, which can be used to run arbitrary code in the context of the current user.

Specific file system drivers could also trigger the vulnerability if characters that do match the reserved characters from the Windows naming convention are encoded and processed on the vulnerable function.

IOActive has developed a proof-of-concept Unicode exploit that overwrites the saved return address with arbitrary data sent by a modified SMB server. Depending on how the target file system orders files to process, this scenario could be used to attempt putting many user controlled file names at a predetermined location in the memory of the running process to then overwrite the program counter for achieving a more reliable and precise exploitation.

Affected Products

The following versions of Windows were confirmed by Microsoft to be vulnerable. Earlier versions of Windows that are no longer supported may also be affected:

- Windows XP Service Pack 3
- Windows XP Professional x64 Edition Service Pack 2
- Windows Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for Itanium-based Systems Service Pack 2
- Windows 7 for 32-bit Systems
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for Itanium-based Systems
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 R2 for x64-based Systems
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows 8 Release Preview
- Windows Server 2012 Release Candidate

Remediation

Security updates are available from Microsoft Update, Windows Update, and from the Microsoft Download Center.

Microsoft recommends that network system administrators and end users who want to install this security update manually apply the update immediately using update management software or by checking for updates using the Microsoft Update service.

- http://technet.microsoft.com/en-us/security/bulletin/ms12-081