Immunity, Inc. Advisory

Disclosure

Vulnerability

LLSSRV: Clarification and correction of information on a public vulnerability

On February 8th , 2005 Microsoft released, as part of their monthly patch cycle, a patch for a vulnerability in the License Logging Service that could lead an attacker to remote code execution (MS05-010). Microsoft claims in their advisory "*For Windows 2000 Server Service Pack 4 and Windows Server 2003, only authenticated users or programs can establish a connection to the License Logging service*".

After conducting follow-up research on this vulnerability Immunity Inc. has discovered that **Windows 2000 Advanced Server and Server which include Service Pack 4 on the CD** have the "llsrpc" Named Pipe listed in the HKLM\SYSTEM\ControlSet001\Services\lanmanserver\parameters\NullSessionPipes registry value (MULTI_SZ) thus meaning that any remote user can bind and send requests to it without any authentication.

Further research lead to Immunity Inc. exploiting two consecutive buffer overflows which are accessed through the LlsrLicenseRequestW RPC function. These overflows are present in the **RegistryDisplayNameGet** and **RegistryFamilyDisplayNameGet** functions which calls lstrcpyW with user supplied source strings allowing the copying of unchecked amount of bytes into a static buffer located in the .data segment of the binary.

Affected

Windows 2000 Advanced Server and Windows 2000 Server which included Service Pack 4 on the install CD
(See http://www.microsoft.com/technet/security/Bulletin/MS05-010.mspx)

Not Affected

Windows 2000 Server and Advanced Server which had Service Pack 4 manually installed.

Detection

Immunity research currently provides a reliable cross-language exploit in CANVAS for both Windows 2000 Advanced Server SP 4 and Windows NT 4.0 SP 6a.

For questions or comments, please contact Immunity, Inc. at admin@immunitysec.com, or http://www.immunitysec.com.

History

Research into this issue was conducted by Immunity Researchers Sinan Eren sinan.eren@immunitysec.com and Nicolas Waisman nicolas.waisman@immunitysec.com

February 2005 - manual binary audit, bug discovery.

February 2005 - POC development, released to Immunity Vulnerability Sharing Club (http://www.immunitysec.com/services-sharing.shtml)

March 16, 2005 – Released to public