

MinorRev: Microsoft Security Bulletin MS05-010 – Vulnerability in the License Logging Service Could Allow Code Execution (885834)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-04/0022.html>

From: Russ Cooper (*Russ.Cooper_at_TRUSECURE.CA*)

Date: 04/12/05

Date: Tue, 12 Apr 2005 13:34:11 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Microsoft Security Bulletin MS05-010:
Vulnerability in the License Logging Service Could Allow Code Execution (885834)

Bulletin URL:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-010.msp>>

Reason for Revision: Bulletin updated to reflect a revised 'Mitigating Factors' section for Windows 2000 Server Service Pack 4. This update documents a known issue with a mitigating factor and the availability of Microsoft Knowledge Base Article 896589.

Version Number: 1.2

Issued Date: Tuesday, February 08, 2005

Revision Date: Tuesday, April 12, 2005

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

Patch(es) Replaced: None

Caveats: Microsoft Knowledge Base Article 885834 documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see Microsoft Knowledge Base Article 885834.

Tested Software:

Affected Software:

* Microsoft Windows NT Server 4.0 Service Pack 6a

<<http://tinyurl.com/6hrxp>>

* Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

<<http://tinyurl.com/4asr6>>

* Microsoft Windows 2000 Server Service Pack 3 and Microsoft Windows 2000 Server Service Pack 4

<<http://tinyurl.com/637j8>>

* Microsoft Windows Server 2003

<<http://tinyurl.com/57yn7>>

* Microsoft Windows Server 2003 for Itanium-based Systems Windows Server 2003 (all versions)

<<http://tinyurl.com/6wdf9>>

Technical Description:

* License Logging Service Vulnerability – CAN-2005-0050 A remote code execution vulnerability exists in the License Logging service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

Revision History:

- * v1.0 – 2/8/2005: Bulletin published
* v1.1 – 2/23/2005: Bulletin updated to reflect a revised 'Security Update Information' section for Windows Server 2003 Microsoft Knowledge Base Article 896589
* v1.2 – 4/12/2005: Bulletin updated to reflect a revised 'Mitigating Factors' section for Windows 2000 Server Service Pack 4. This update documents a known issue with a mitigating factor and the availability of Microsoft Knowledge Base Article 896589.

This email is sent to NTBugtraq automatically as a service to my subscribers. (v4.01.1928.12470)

Cheers,

Russ Cooper – Senior Scientist – Cybertrust/NTBugtraq Editor

--

NTBugtraq Editor's Note:

Most viruses these days use spoofed email addresses. As such, using an Anti-Virus product which a

--