

Securiteam: [NT] Vulnerability in the License Logging Service Allows Code Execution (MS05-010)

[NT] Vulnerability in the License Logging Service Allows Code Execution (MS05-010)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0027.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/09/05

To: list@securiteam.com

Date: 9 Feb 2005 18:28:42 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.secureteam.com/maillinglist.html>

Vulnerability in the License Logging Service Allows Code Execution
(MS05-010)

SUMMARY

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.

DETAILS

Affected Software:

Microsoft Windows NT Server 4.0 Service Pack 6a –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=817FDC2D-AEE2-4FAF-908B-197B65A471F2>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=F7B0934C-3049-4B01-956A-B116F69A667E>>

Download the update

Microsoft Windows 2000 Server Service Pack 3 and Microsoft Windows 2000

Server Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E9983AA2-2CEC-4B62-80D6-8E966A83A5D1>>

Download the update

Microsoft Windows Server 2003 –

Securiteam: [NT] Vulnerability in the License Logging Service Allows Code Execution (MS05-010)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=06EAF8E3-CCB7-482B-8B68-340521150113>>

Download the update

Microsoft Windows Server 2003 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=EC25EC00-9C08-4555-94C7-21D5A521FDB6>>

Download the update

Non-Affected Software:

- * Microsoft Windows 2000 Professional Service Pack 3 and Microsoft Windows 2000 Professional Service Pack 4
- * Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
- * Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)
- * Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)
- * Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

CVE Information:

License Logging Service Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0050>>

CAN-2005-0050

Mitigating Factors:

- * On Windows Server 2003 the License Logging service is disabled by default. Typically only administrators can change the startup type of a service. An attacker would first have to change the startup type from Disabled, and then start the service to try to exploit this vulnerability. If the License Logging service is manually started on Windows Server 2003, attempts to exploit this vulnerability could cause in a denial of service for the affected service. This vulnerability does not allow remote code execution on Windows Server 2003.
- * On Small Business Server 2000 and on Windows Small Business Server 2003, the License Logging service is installed and running. However, by default, on Windows Small Business Server 2003 and earlier, the License Logging service communication ports are blocked from the Internet and the License Logging service is available only on the local network.
- * On Windows 2000 Server Service Pack 4 and Windows Server 2003, only authenticated users or programs can establish a connection to the License Logging service.
- * Disabling the License Logging service helps prevent the possibility of a remote attack. Customers that have disabled this service would be at a reduced risk to attack from this vulnerability. See the Workarounds section for instructions that describe how to disable this service. By default, affected operating systems other than Windows Server 2003 have the License Logging service startup type set to Automatic instead of Disabled.

*

<<http://www.microsoft.com/TECHNET/SECURITY/PRODTECH/WIN2000/SECWIN2K/DEFAULT.MSPX>>

Chapter 6 of Microsoft Solution for Securing Windows 2000 Server, Hardening the Base Windows 2000 Server recommends disabling the License Logging service. Environments that comply with these guidelines could be at a reduced risk from this vulnerability.

- * Firewall best practices and standard default firewall configurations

Securiteam: [NT] Vulnerability in the License Logging Service Allows Code Execution (MS05-010)

can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports

Workarounds:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

* Disable the License Logging service:

Disabling the License Logging service will help protect from remote attempts to exploit this vulnerability.

Note Do not perform this procedure on Small Business Server 2000 or Windows Small Business Server 2003. These operating system versions require the License Logging service. These operating system versions may fail to function correctly if the License Logging service is disabled.

You can disable the License Logging service services by following these steps:

1. Click Start, and then click Control Panel (or point to Settings, and then click Control Panel).
2. Double-click Administrative Tools.
3. Double-click Services.
4. Double-click License Logging Service.
5. In the Startup type list, click Disabled.
6. Click Stop, and then click OK.

Impact of Workaround: If the License Logging service is disabled, any services that explicitly depend on the License Logging services may log an error message in the system event log. For more information, see <http://support.microsoft.com/kb/316631> Microsoft Knowledge Base Article 316631.

* Use the Group Policy settings to disable License Logging Service on all affected systems that do not require this feature.

Because the License Logging service is a possible attack vector, disable it by using the Group Policy settings. You can disable the startup of this service at the local, site, domain, or organizational unit level by using Group Policy object functionality in Windows 2000 domain environments or in Windows Server 2003 domain environments.

Note Do not perform this procedure on Small Business Server 2000 or Windows Small Business Server 2003. These operating system versions require the License Logging service. These operating system versions may fail to function correctly if the License Logging service is disabled.

Note You may also review the

<http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&Di> Windows 2000 Security Hardening Guide. This guide includes information about how to disable services.

For more information about Group Policy, visit the following Web sites:

*

Securiteam: [NT] Vulnerability in the License Logging Service Allows Code Execution (MS05-010)

<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep>
Step-by-Step Guide to Understanding the Group Policy Feature Set

*

<<http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp>> Windows
2000 Group Policy

*

<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/gp/default.mspx>>
Group Policy in Windows Server 2003

Impact of Workaround: If the License Logging service is disabled, any services that explicitly depend on the License Logging service may log an error message in the system event log. For more information, see <<http://support.microsoft.com/kb/316631>> Microsoft Knowledge Base Article 316631.

* On Windows NT Server 4.0 Service Pack 6a, Windows NT Server 4.0 Terminal Server Edition Service Pack 6, and Windows 2000 Server Service Pack 3 remove the License Logging service from the NullSessionPipes registry key:

Affected operating systems that are earlier than Windows 2000 Server Service Pack 4 allowed anonymous connections to the License Logging service. Removing the License Logging service from the NullSessionPipes subkey registry key will help prevent attempts to exploit this vulnerability by an anonymous attacker. This workaround will not prevent attacks from authenticated users and should only be used if the License Logging service cannot be disabled. For more information about this change, see <<http://support.microsoft.com/kb/815458>> Microsoft Knowledge Base Article 815458.

Note Using Registry Editor incorrectly can cause serious problems that may require that you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. For information about how to modify the registry, view the "Change Keys And Values" Help topic in Registry Editor (Regedit.exe) or view the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe.

Note We recommend backing up the registry before you modify it.

1. Click Start, click Run, type "regedt32" (without the quotation marks), and then click OK.
2. In Registry Editor, locate the following registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes
3. Edit the registry key and remove the Llsrpc value.
4. Restart the affected system after performing these actions.

Impact of Workaround: Anonymous connections to the License Logging service will not be allowed. There is no known impact of this change. This is the default configuration of Windows 2000 Server Service Pack 4.

* Use a personal firewall, such as the

<<http://go.microsoft.com/fwlink/?LinkId=33335>> Internet Connection

Securiteam: [NT] Vulnerability in the License Logging Service Allows Code Execution (MS05-010)

Firewall, which is included with Windows Server 2003.

By default, the Internet Connection Firewall feature in Windows Server 2003 helps protect your Internet connection by blocking unsolicited incoming traffic. We recommend that you block all unsolicited incoming communication from the Internet.

Note Do not perform this procedure on Small Business Server 2000 or Windows Small Business Server 2003. Use the instructions provided in the Run the Configure E-mail and Internet Connection Wizard workaround instead of this procedure.

To enable the Internet Connection Firewall feature by using the Network Setup Wizard, follow these steps:

1. Click Start, and then click Control Panel.
2. In the default Category View, click Network and Internet Connections, and then click Setup or change your home or small office network. The Internet Connection Firewall feature is enabled when you select a configuration in the Network Setup Wizard that indicates that your system is connected directly to the Internet.

To configure Internet Connection Firewall manually for a connection, follow these steps:

1. Click Start, and then click Control Panel.
2. In the default Category View, click Networking and Internet Connections, and then click Network Connections.
3. Right-click the connection on which you want to enable Internet Connection Firewall, and then click Properties.
4. Click the Advanced tab.
5. Click to select the Protect my computer or network by limiting or preventing access to this computer from the Internet check box, and then click OK.

Note If you want to enable certain programs and services to communicate through the firewall, click Settings on the Advanced tab, and then select the programs, the protocols, and the services that are required.

* Block TCP ports 139 and 445 at the firewall:

These ports are used to initiate a connection with the License Logging service using named pipe connections. Blocking them at the firewall will help prevent systems that are behind that firewall from attempts to exploit this vulnerability. We recommend that you block all unsolicited inbound communication from the Internet to help prevent attacks that may use other ports. For more information about ports, visit the following Web site.

* Run the Configure E-mail and Internet Connection Wizard
Small Business Server 2000 and Windows Small Business Server 2003 include firewall technology that helps protect your Internet connection by blocking unsolicited incoming traffic. The firewall technology in Small Business Server 2000 and Windows Small Business Server 2003 is configured automatically when you run the Configure E-mail and Internet Connection

Wizard.

To configure the firewall technology using the Configure E-mail and Internet Connection Wizard, follow these steps:

1. Click Start, and then click Server Management.
 2. In the console tree, click Internet and E-mail
- In the details pane, click Connect to the Internet.

1. Accept the default values in the wizard.

* Enable advanced TCP/IP filtering on systems that support this feature. You can enable advanced TCP/IP filtering to block all unsolicited inbound traffic. For more information about how to configure TCP/IP filtering, see <<http://support.microsoft.com/kb/309798>> Microsoft Knowledge Base Article 309798.

* Block the affected ports by using IPSec on the affected systems. Use Internet Protocol security (IPSec) to help protect network communications. Detailed information about IPSec and about how to apply filters is available in <<http://support.microsoft.com/kb/313190>> Microsoft Knowledge Base Article 313190 and <<http://support.microsoft.com/kb/813878>> Microsoft Knowledge Base Article 813878.

Frequently Asked Questions:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could remotely take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

On Windows Server 2003, the most likely attack scenario is a denial of service. An attacker who successfully exploited this vulnerability could cause the License Logging service to fail on Windows Server 2003. Restarting the License Logging service allows the service to function correctly. However, the License Logging service could remain vulnerable to another denial of service attack.

On Windows 2000 Server Service Pack 4 and Windows Server 2003, only authenticated users or programs can establish a connection to the License Logging service.

What causes the vulnerability?

An unchecked buffer in the License Logging service.

What is the License Logging service?

The License Logging service is a tool that was originally designed to help customers manage licenses for the Microsoft server products that are licensed in the Server Client Access License (CAL) model. License Logging service is one of the services used by Windows Small Business Server 2003 or earlier to manage CALs. By default, the License Logging service is disabled in Windows Server 2003. The License Logging service will not be included in future versions of the Windows operating system. For more information about the License Logging service, see

<<http://support.microsoft.com/kb/842196>> Microsoft Knowledge Base Article 842196.

How do I know if I use the License Logging service on my server?

The License Logging service is not available on Windows 2000 Professional or Windows XP. By default, the License Logging service is installed and running on Windows NT Server 4.0, on Windows NT Server 4.0 Terminal Server Edition, and on Windows 2000 Server. By default, the License Logging service is installed but not running on Windows Server 2003. By default, the License Logging service is installed and running on Small Business Server 2000 and on Windows Small Business Server 2003. You can determine if the License Logging service is installed by following this procedure. These steps apply only to Windows 2000 and later versions. For Windows NT 4.0, follow the procedure that is included in the product documentation.

To verify the License Logging service:

1. Click Start, click Programs, click Administrative Tools, and then click Services.
2. Verify that the License Logging service is present.
3. If the License Logging service is running, follow the instructions in the Workarounds section of this security bulletin to disable the service.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take complete control of the affected system. The vulnerability, if exploited, could allow an attacker to cause the License Logging service on Windows Server 2003 to stop responding to all requests.

Who could exploit the vulnerability?

On Windows NT Server 4.0 Service Pack 6a, Windows NT Server 4.0 Terminal Server Edition Service Pack 6, and Windows 2000 Server Service Pack 3 any anonymous user who could establish a connection with an affected system by using the affected ports could attempt to exploit this vulnerability.

On Windows 2000 Server Service Pack 4 and Windows Server 2003, only authenticated users or programs can establish a connection to the License Logging service.

On Small Business Server 2000 running on Windows 2000 Server Service Pack 3, any anonymous user who could establish a connection with an affected system by using the affected ports could attempt to exploit this vulnerability. On Windows Small Business Server 2003 and Small Business Server 2000 running on Windows 2000 Server Service Pack 4, only authenticated users or programs on the local network can establish a connection to the License Logging service.

How could an attacker exploit the vulnerability?

An attacker could attempt to exploit this vulnerability by creating a specially-crafted network message and by sending the message to the affected system. On Windows Server 2003, receipt of such a message could cause the service to fail causing a denial of service.

Securiteam: [NT] Vulnerability in the License Logging Service Allows Code Execution (MS05-010)

What systems are primarily at risk from the vulnerability?

Windows NT Server 4.0 Service Pack 6a, Windows NT Server 4.0 Terminal Server Edition Service Pack 6, and Windows 2000 Server are primarily at risk from this vulnerability.

Windows 2000 Professional and Windows XP are not at risk from this vulnerability. Windows Server 2003 is impacted at a lower severity rating partly because the License Logging service startup type is set to Disabled. An attacker would first have to change the setting from Disabled to Manual or Automatic, and then start the service to attempt to remotely exploit this vulnerability. Typically, only administrators can change the startup type of a service. Operating systems other than Windows Server 2003 have the License Logging service set to a startup type of Automatic instead of Disabled. After the License Logging service is started, the affected system could be vulnerable to a remote attack. To help prevent this, see the Workarounds section for instructions that explain how you can disable the License Logging service.

Could the vulnerability be exploited over the Internet?

Yes. An attacker could try to exploit this vulnerability over the Internet. Firewall best practices and standard default firewall configurations can help protect against attacks that originate from the Internet. Microsoft has provided information about how you can help protect your PC. End users can visit the <http://go.microsoft.com/fwlink/?LinkId=21169> Protect Your PC Web site. IT professionals can visit the <http://go.microsoft.com/fwlink/?LinkId=21171> Security Guidance Center Web site.

What does the update do?

The update removes the vulnerability by modifying the way that the License Logging service validates the length of a message before it passes the message to the allocated buffer.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

ADDITIONAL INFORMATION

Securiteam: [NT] Vulnerability in the License Logging Service Allows Code Execution (MS05-010)

The original article can be found at:

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

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

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.