

# [NT] Buffer Overrun in Messenger Service Could Allow Code Execution (MS03-043)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0068.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 10/16/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 16 Oct 2003 14:37:16 +0200

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

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

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

-----

Buffer Overrun in Messenger Service Could Allow Code Execution (MS03-043)

---

## SUMMARY

A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. The vulnerability results because the Messenger Service does not properly validate the length of a message before passing it to the allocated buffer.

## DETAILS

### Vulnerable Systems:

- \* Microsoft Windows NT Workstation 4.0, Service Pack 6a
- \* Microsoft Windows NT Server 4.0, Service Pack 6a
- \* Microsoft Windows NT Server 4.0, Terminal Server Edition, Service Pack 6
- \* Microsoft Windows 2000, Service Pack 2
- \* Microsoft Windows 2000, Service Pack 3, Service Pack 4
- \* Microsoft Windows XP Gold, Service Pack 1
- \* Microsoft Windows XP 64-bit Edition
- \* Microsoft Windows XP 64-bit Edition Version 2003
- \* Microsoft Windows Server 2003
- \* Microsoft Windows Server 2003 64-bit Edition

## Securiteam: [NT] Buffer Overrun in Messenger Service Could Allow Code Execution (MS03-043)

### Immune Systems:

- \* Microsoft Windows Millennium Edition

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0717>>

CAN-2003-0717

The software listed above has been tested to determine if the versions are affected. Other versions are no longer

<<http://support.microsoft.com/directory/discontinue.asp>> supported, and may or may not be affected.

### Patch Availability:

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7597FCF4-6615-4074-9E46-A17D808ED38D&dis>  
Microsoft Windows NT Workstation 4.0, Service Pack 6a

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B1949456-996A-485A-9A28-79FD79F26A1B&dis>  
Microsoft Windows NT Server 4.0, Service Pack 6a

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=64AB4B66-1A6E-4264-93A8-26CDB98B05A8&dis>  
Microsoft Windows NT Server 4.0, Terminal Server Edition, Service Pack 6

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=A0061377-1683-4C13-9527-5534F6C7CF85&displa>  
Microsoft Windows 2000, Service Pack 2

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=99F1B40D-906A-4945-A021-4B494CCCBDE0&dis>  
Microsoft Windows 2000, Service Pack 3, Service Pack 4

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=F02DA309-4B0A-4438-A0B9-5B67414C3833&dis>  
Microsoft Windows XP Gold, Service Pack 1

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=2BE95254-4C65-4CA5-80A5-55FDF5AA2296&dis>  
Microsoft Windows XP 64-bit Edition

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8B990946-84C8-4C91-899C-5A44EC13174E&displ>  
Microsoft Windows XP 64-bit Edition Version 2003

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1DF106F3-7EC4-4EB0-9143-C1E3C9E2F5F8&dis>  
Microsoft Windows Server 2003

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8B990946-84C8-4C91-899C-5A44EC13174E&displ>  
Microsoft Windows Server 2003 64-bit Edition

An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. The attacker could then take any action on the system, including installing programs, viewing, changing or deleting data, or creating new accounts with full privileges.

### Mitigating factors:

- \* Messages are delivered to the Messenger service via NetBIOS or RPC. If

## Securiteam: [NT] Buffer Overrun in Messenger Service Could Allow Code Execution (MS03-043)

users have blocked the NetBIOS ports (ports 137–139) – and UDP broadcast packets using a firewall, others will not be able to send messages to them on those ports. Most firewalls, including Internet Connection Firewall in Windows XP, block NetBIOS by default.

\* Disabling the Messenger Service will prevent the possibility of attack.

\* On Windows Server 2003 systems, the Messenger Service is disabled by default.

### Workarounds:

Microsoft has tested the following workarounds. These workarounds will not correct the underlying vulnerability however they help block known attack vectors. Workarounds may cause a reduction in functionality in some cases – in such situations this is identified below.

Use a personal firewall such as

<<http://www.microsoft.com/security/protect/windowsxp/firewall.asp>>

Internet Connection Firewall (only available on XP and Windows Server 2003).

If you are using the Internet Connection Firewall in Windows XP or Windows Server 2003 to protect your Internet connection, it will by default block inbound RPC traffic from the Internet.

To enable Internet Connection Firewall feature using the Network Setup Wizard:

1. Run the Network Setup Wizard. To access this wizard, point to Control Panel, double-click Network and Internet Connections, and then click Setup or change your home or small office network.
2. The Internet Connection Firewall is enabled when you choose a configuration in the wizard that indicates that your computer is connected directly to the Internet.

To configure Internet Connection Firewall manually for a connection:

1. In Control Panel, double-click Networking and Internet Connections, and then click Network Connections.
2. Right-click the connection on which you would like to enable ICF, and then click Properties.
3. On the Advanced tab, click the box to select the option to Protect my computer or network.
4. If you want to enable the use of some applications and services through the firewall, you need to enable them by clicking the Settings button, and then selecting the programs, protocols, and services to be enabled for the ICF configuration.

### Disable the Messenger Service

Disabling the messenger service will prevent the possibility of an attack.

You can disable the messenger service by performing the following:

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 Messenger.
5. In the Startup type list, click Disabled.
6. Click Stop, and then click OK.

## Securiteam: [NT] Buffer Overrun in Messenger Service Could Allow Code Execution (MS03-043)

### Impact of Workaround:

If the Messenger service is disabled, messages from the Alerter service (for example notifications from your backup software or Uninterruptible Power Supply) are not transmitted. If the Messenger service is disabled, any services that explicitly depend on the Messenger service do not start, and an error message is logged in the System event log.

### Frequently Asked Questions

#### What's the scope of the vulnerability?

This is a buffer overrun vulnerability. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. The attacker could then be able to take any action on the system, including installing programs, viewing, changing or deleting data, or creating new accounts with full privileges.

#### What is the Windows Messenger Service?

The Messenger service is a Windows service that transmits net send messages and messages that are sent through the Alerter service between client computers and servers. For example, the Messenger service can be used by network administrators to send administrative alerts to network users. The Messenger service can also be used by Windows and other software programs. For example, Windows may use it to inform you when a print job is completed or when you lose power to your computer and switch to a Uninterruptible Power Supply (UPS). The Messenger service is not related to your Web browser, e-mail program, Windows Messenger, or MSN Messenger.

#### What causes the vulnerability?

The vulnerability results because of an unchecked buffer in the Messenger Service. If exploited, an attacker could gain Local System privileges on an affected system, or cause the service to fail.

#### Is the Messenger Service the same thing as Windows Messenger or MSN Messenger?

No. It's important to note that the Messenger Service is not the same thing as Windows Messenger or MSN Messenger. Windows Messenger ( <<http://messenger.microsoft.com>> <http://messenger.microsoft.com>) and MSN Messenger ( <<http://messenger.msn.com>> <http://messenger.msn.com>) are instant messaging services that allow users to converse, share pictures, video, etc. In contrast, the Messenger service ( <<http://support.microsoft.com/default.aspx?scid=KB:EN-US:168893&>> <http://support.microsoft.com/default.aspx?scid=KB:EN-US:168893&>) is a simple text-only broadcast service that's typically used by administrators to send alerts to users, and warn them of pending outages, server maintenance, etc.

#### What's wrong with the Messenger Service?

The vulnerability results because the Messenger Service does not properly validate the length of a message before passing it to the allocated buffer.

Securiteam: [NT] Buffer Overrun in Messenger Service Could Allow Code Execution (MS03-043)

What could this vulnerability enable an attacker to do?

An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. The attacker could then take any action on the system, including installing programs, viewing, changing or deleting data, or creating new accounts with full privileges.

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by creating a specially crafted message and sending it to the Messenger Service on an affected system.

What does the patch do?

The patch eliminates the vulnerability by insuring that the Messenger Service properly validates the length of a message before passing it to the allocated buffer.

Microsoft thanks the following for working with us to protect customers:

\* The Last Stage of Delirium Research Group for reporting the issue in MS03-043.

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS03-043.asp>>  
<http://www.microsoft.com/technet/security/bulletin/MS03-043.asp>

=====

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.