

# [NT] Buffer Overrun in the ListBox and in the ComboBox Control Could Allow Code Execution (MS03-045)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0065.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 14:41:33 +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 the ListBox and in the ComboBox Control Could Allow Code Execution (MS03-045)  
-----

## SUMMARY

A vulnerability exists because the ListBox control and the ComboBox control both call a function, which is located in the User32.dll file, that contains a buffer overrun. The function does not correctly validate the parameters that are sent from a specially-crafted Windows message. Windows messages provide a way for interactive processes to react to user events (for example, keystrokes or mouse movements) and to communicate with other interactive processes. A security vulnerability exists because the function that provides the list of accessibility options to the user does not correctly validate Windows messages that are sent to it. One process in the interactive desktop could use a specific Windows message to cause the ListBox control or the ComboBox control to execute arbitrary code. Any program that implements the ListBox control or the ComboBox control could allow code to be executed at an elevated level of administrative credentials, as long as the program is running at an elevated level of privileges (for example, Utility Manager in Windows 2000). This could include third-party applications.

## 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

### Immune Systems:

- \* Microsoft Windows Millennium Edition

### Patch Availability:

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=5EA88ABE-8D53-4E25-959C-E80EB5FD7A91&display=details>>  
Microsoft Windows NT Workstation 4.0, Service Pack 6a

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=F3E87075-AAE5-49F4-9D37-24A116296188&display=details>>  
Microsoft Windows NT Server 4.0, Service Pack 6a

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0ADC8D90-2355-49A0-976B-57281B4521C1&display=details>>  
Microsoft Windows NT Server 4.0, Terminal Server Edition, Service Pack 6

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=01358EAC-F1C5-4CB7-BE3D-64459F4AD3FD&display=details>>  
Microsoft Windows 2000, Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=ABC764AC-5B7B-4B99-BF3E-F57352E4C507&display=details>>  
Microsoft Windows 2000 Service Pack 3, Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=ABC764AC-5B7B-4B99-BF3E-F57352E4C507&display=details>>  
Microsoft Windows XP Gold, Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3E7B03BF-2231-4069-B76F-0BD69CF6E1D9&display=details>>  
Microsoft Windows XP 64 bit Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E4BD7C05-EA0E-49C7-9BDD-ABB496CA87CA&display=details>>  
Microsoft Windows XP 64 bit Edition Version 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=02F97DE4-29DF-4D33-A33B-E7630349E69E&display=details>>  
Microsoft Windows Server 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E4BD7C05-EA0E-49C7-9BDD-ABB496CA87CA&display=details>>  
Microsoft Windows Server 2003 64 bit Edition

## Securiteam: [NT] Buffer Overrun in the ListBox and in the ComboBox Control Could Allow Code Execution (MS03-04)

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

<<http://www.microsoft.com/exchweb/bin/redirect.asp?URL=http://support.microsoft.com/directory/discontinue.asp>> supported, and may or may not be affected.

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0659>>  
CAN-2003-0659

An attacker who had the ability to log on to a system interactively could run a program that could send a specially-crafted Windows message to any applications that have implemented the ListBox control or the ComboBox control, causing the application to take any action an attacker specified.

This could give an attacker complete control over the system by using Utility Manager in Windows 2000.

### Mitigating factors:

- \* An attacker must have valid logon credentials to exploit the vulnerability. The vulnerability could not be exploited remotely.

- \* Properly-secured systems are at little risk from this vulnerability.

Standard best practices recommend only allowing trusted users to log on to systems interactively.

- \* Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 are affected by this vulnerability in the ListBox control and in the ComboBox control. However, in Windows XP and in Windows Server 2003, Utility Manager runs under the context of the logged-on user and does not allow for elevation of privileges. Windows NT 4.0 does not implement Utility Manager.

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.

- \* Disable the Utility Manager on all affected systems that do not need this feature through software policies

- \* Since the Utility Manager Service is a possible attack vector this can be disabled using software restriction policies within Active Directory or within the Local Security Policy. The Utility Manager process name is utilman.exe. You may use the following software restriction policy guides to help prevent users from accessing this file:

<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/maintain/rstrplcy.asp>>

Using Software Restriction Policies to Protect Against Unauthorized Software

<<http://support.microsoft.com/default.aspx?scid=kb:en-us:324036>> HOW TO:

Use Software Restriction Policies in Windows Server 2003 (324036)

<<http://www.microsoft.com/windowsxp/pro/evaluation/overviews/antivirus.asp>> Protect Your System from Viruses (Using Software Restriction Policies)

[<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standards/>](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standards/)

To create new software restriction policies

#### Impact of Vulnerability:

The Utility Manager Service provides many of the accessibility features of the operating system. These would be unavailable until the restrictions are removed.

#### Frequently Asked Questions

What is the scope of the vulnerability?

This is a buffer overrun vulnerability. An attacker who successfully exploited this vulnerability on Windows 2000 could gain complete control over a system. This would give the attacker the ability to take any action that they want on a system such as adding, deleting, or modifying data. It could also give the attacker the ability to create or to delete user accounts, or to add accounts to the local administrators group.

The vulnerability could only be exploited by an attacker who has credentials to log on to the computer interactively. Since restricted users are not normally permitted to logon to mission critical server this vulnerability primarily of concern on workstations and terminal servers. Any application that has implemented the ListBox control or the ComboBox control, which is in the User32.dll file, could allow code to be executed at an elevated level of privileges, as long as the program is running at an elevated level of privileges (for example, the Utility Manager utility in Windows 2000). This could include third-party applications.

What causes the vulnerability?

A vulnerability results because the ListBox control and the ComboBox control both call a function, which is located in the User32.dll file, that contains a buffer overrun. The function does not correctly validate the parameters that are sent from a specially-crafted Windows message.

What is Utility Manager?

Utility Manager is an accessibility utility that allows users to check the status of accessibility programs (for example, Microsoft Magnifier, Narrator, or On-Screen Keyboard) and to start or to stop them.

What are Windows messages?

Processes that run on Windows interact with the system and other processes by using messages. For example, each time the user presses a key on the keyboard, moves the mouse, or clicks a control such as a scroll bar, Windows generates a message. The purpose of this message is to alert the program that a user event has occurred and to deliver the data from that event to the program. Similarly, a program can generate messages to allow the various windows that it controls to communicate with each other.

What is wrong with the way that Windows messages are handled by the ListBox control?

The vulnerability lies in the way that the function that both the ListBox control and the ComboBox control use to handle messages when the controls present the list of available accessibility functions to the user. The

function that is called does not correctly validate Windows messages that are sent to it. When Utility Manager is running on Windows 2000, another process could run on the system and could send a specially-crafted message to Utility Manager. In Windows 2000, Utility Manager runs under the context of the Local System. This context has a higher level of administrative credentials than a logged-on user and could allow arbitrary code to be executed.

Why does this pose a security vulnerability?

The vulnerability in the ListBox control and in the ComboBox control could provide a way for a process to cause Utility Manager to run arbitrary code on Windows 2000. Although it is against best practice guidelines, a third-party application could use the ListBox control or in the ComboBox control under the context of the Local System.

What might an attacker use the vulnerability to do?

To exploit this vulnerability an attacker would first have to start Utility Manager on Windows 2000 and then could run a specially-designed application that could exploit the vulnerability in the ListBox control and the ComboBox control. In default configurations of Window 2000, Utility Manager is installed but is not running. This vulnerability could allow an attacker to gain complete control over the system on Windows 2000.

Who could exploit the vulnerability?

To exploit the vulnerability, an attacker must be able to log on to the system, start Utility Manager, and execute a program that sends a specially-crafted message to Utility Manager that exploits the vulnerability.

What versions of the ListBox control or of the ComboBox control are vulnerable to this attack?

Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 are affected by this vulnerability. However, the Windows XP and Windows Server 2003 versions of Utility Manager do not allow elevation of permissions because Utility Manager runs under the context of the logged-on user. Windows NT 4.0 does not implement Utility Manager however the vulnerable function is still present within User32.dll.

I'm using Windows 2000, but I'm not using Utility Manager or any of the accessibility features, am I still vulnerable?

Yes – Utility Manager is installed and enabled by default.

Which systems are primarily at risk from the vulnerability?

Workstations and terminal servers are primarily at risk. Servers are only at risk if users who do not have sufficient administrative credentials are given the ability to log on to servers and to run programs. However, best practices strongly discourage allowing this.

Could the vulnerability be exploited over the Internet?

No. The attacker must be able to log on to the specific system that they

Securiteam: [NT] Buffer Overrun in the ListBox and in the ComboBox Control Could Allow Code Execution (MS03-045)

want to attack. The attacker cannot load and run a program remotely.

What does the patch do?

The patch addresses the vulnerability by changing way that the function used by the ListBox control and the ComboBox control use to handle Windows messages so that the parameters that are passed are correctly validated.

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

Brett Moore of <<http://www.security-assessment.com>>

Security-Assessment.com for reporting the issue in MS03-045.

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS03-045.asp>>

<http://www.microsoft.com/technet/security/bulletin/MS03-045.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.