

[NT] Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0040.html>

From: support@securiteam.com

Date: 04/21/03

From: support@securiteam.com

To: list@securiteam.com

Date: 21 Apr 2003 13:45:24 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges

SUMMARY

The Windows kernel is the core of the operating system. It provides system level services such as device and memory management, allocates processor time to processes, and manages error handling.

There is a flaw in the way the kernel passes error messages to a debugger. A vulnerability results because an attacker could write a program to exploit this flaw and run code of their choice. An attacker could exploit this vulnerability to take any action on the system including deleting data, adding accounts with administrative access, or reconfiguring the system.

For an attack to be successful, an attacker would need to be able to logon interactively to the system, either at the console or through a terminal session. In addition, a successful attack would require the introduction of code in order to exploit this vulnerability. Because best practices, recommends restricting the ability to logon interactively on servers, this

Securiteam: [NT] Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges

issue most directly affect client systems and terminal servers.

DETAILS

Affected Software:

- * Microsoft Windows NT 4.0
- * Microsoft Windows NT 4.0 Server, Terminal Server Edition
- * Microsoft Windows 2000
- * Microsoft Windows XP

Mitigating factors:

- * A successful attack requires the ability to logon interactively to the target machine, either directly at the console or through a terminal session.
- * Properly secured servers would be at little risk from this vulnerability. Standard best practices recommend only allowing trusted administrators to log onto such systems interactively; without such privileges, an attacker could not exploit the vulnerability.

Patch availability:

Download locations for this patch

- * Windows NT 4.0:

*

<http://microsoft.com/downloads/details.aspx?FamilyId=C3596ED1-596F-416C-8BE5-91AE65619A1A&displaylang=en>

All except Japanese NEC and Chinese – Hong Kong

*

<http://microsoft.com/downloads/details.aspx?FamilyId=6D83F8BA-BF16-4EC5-9187-9B03E9AE825F&displaylang=ja>

Japanese NEC

*

<http://microsoft.com/downloads/details.aspx?FamilyId=0FF5C348-F7A0-44E8-8D82-557389FB4590&displaylang=zh>

Chinese – Hong Kong

- * Windows NT 4.0, Terminal Server Edition:

*

<http://microsoft.com/downloads/details.aspx?FamilyId=910A0015-3723-4A4E-9049-99A4CE52B5F8&displaylang=en>

All

- * Windows 2000:

*

<http://microsoft.com/downloads/details.aspx?FamilyId=CACAC8C0-81E9-413E-B565-5D7B3257A733&displaylang=en>

All except Japanese NEC

*

<http://microsoft.com/downloads/details.aspx?FamilyId=81E6E80C-5E56-4466-98C1-4DDF6CF3893F&displaylang=ja>

Japanese NEC

- * Windows XP:

*

<http://microsoft.com/downloads/details.aspx?FamilyId=9F81E615-3DEC-4A4B-826A-4E0FEAB42323&displaylang=en>

32-bit Edition

*

<http://microsoft.com/downloads/details.aspx?FamilyId=DBC47904-51C8-475A-9900-3DF363A51A3A&displaylang=en>

64-bit Edition

What's the scope of the vulnerability?

This is a privilege elevation vulnerability. An attacker who has the ability to interactively log on to a system and run code of their choice could seek to exploit this vulnerability and run code of their choice with higher privileges. This could allow an attacker to carry out any action on the system including creating administrative accounts or modifying or deleting data.

Because a successful attack would require the ability for the attacker to logon interactively and run a program, the systems most likely to be affected by this vulnerability are client systems and terminal servers, which regularly allow end-users access to the system directly. Servers such as mail servers, database servers, application servers and file servers are normally configured to restrict the ability of users to log on interactively and therefore are less likely to be affected by this vulnerability.

What causes the vulnerability?

The vulnerability results because of an unchecked buffer used by the Windows kernel for passing error messages to a debugger.

What is the Windows Kernel?

The Windows kernel is the core of the Windows operating system. It provides basic services, such as memory and device management, which all other applications depend upon.

What is a debugger?

A debugger is a software program that provides a way for system administrators and developers to troubleshoot programs running on Windows by interrogating the code that is running on the system directly.

A debugger works by "attaching" to a particular process and then listening for error messages from that process. When an error message is detected, the debugger then displays the error message to allow analysis. The kernel manages the passage of messages to and from a debugger. Windows NT, Windows 2000, and Windows XP include a debugger.

What's wrong with the way the Kernel handles debug messages in Windows?

There is a flaw in the Windows kernel caused by a difference in the permitted size of an outgoing error message, and the size of the buffer that can receive that error message. This means that if an overly large message is passed between the kernel and the debugger, the buffer can be caused to overflow.

The flaw is in the Windows kernel and how it passes messages to the debugger, and not in the debugger itself.

What could this vulnerability enable an attacker to do?

An attacker with sufficient rights to logon interactively could use this

Securiteam: [NT] Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges

vulnerability to run code of their choice. For example, the attacker could execute code that could allow adding accounts with administrative privileges, deleting critical system files, or changing security settings.

It is important to note that an attacker would need to be able to logon interactively to the system. This vulnerability could not be exploited by a remote or an anonymous user.

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by writing a program that would send a number of especially malformed debugger messages to and from the Windows kernel in such a way as to overflow the affected buffer. This could allow the attacker to run code of their choice, which could be used to elevate privilege.

For an attack to be successful, the attacker would need to be able to logon interactively and to introduce hostile code to the system. Best practices suggest that users' ability to logon and load programs should be limited in accordance with the rule of least privilege, which would mitigate the chances for a successful attack.

What does the patch do?

The patch addresses the vulnerability by correctly handling information sent from the Windows kernel to the debugger.

In the Additional Information section below you state that the Windows 2000 patch supercedes the Windows 2000 Patch for MS03-007. Does this patch correct the problem discussed in the Caveats section of MS03-007?

Yes – the problem with MS03-007 was caused by a dependent file not being present in the patch. This file dependency only manifested itself under very specific circumstances – the system needed to be running Windows 2000 Service Pack 2 and have had one of a small number of non-security HotFixes installed – which had to have been obtained from Microsoft Product Support Services.

The Windows 2000 patch for this security vulnerability includes the dependent file, and includes the fix for MS03-007. This means that the patch will install on the systems described above without causing the same issue as the MS03-007 patch.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:0_46831_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com>
Microsoft Product Security.

=====

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

Securiteam: [NT] Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges

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.