

[NT] Vulnerability in Cursor and Icon Format Handling Allows Remote Code Execution (MS05-002)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0052.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/12/05

To: list@securiteam.com

Date: 12 Jan 2005 11:44:06 +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>

Vulnerability in Cursor and Icon Format Handling Allows Remote Code Execution (MS05-002)

SUMMARY

Two newly discovered vulnerabilities in the Windows Operating system allow a remote attacker to compromise the server. One vulnerability involves using malformed Cursor or Icon file, while the other involves an attack against the Windows' Kernel via again a malformed Cursor or Icon file.

DETAILS

Affected Software:

* Microsoft Windows NT Server 4.0 Service Pack 6a

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=4604400A-287E-48CC-91B1-BEE44EEA588C>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=94A0B521-4C39-4D15-AA80-068C30476E6F>>

Download the update

* Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000

Service Pack 4

Securiteam: [NT] Vulnerability in Cursor and Icon Format Handling Allows Remote Code Execution (MS05-002)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=722C6C65-3F6C-4029-8EB7-D4612A785E78>>

Download the update

- * Microsoft Windows XP Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8850954D-57D9-4D23-9AA1-1CCF6085A057>>

Download the update

- * Microsoft Windows XP 64-Bit Edition Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=2325700F-7931-4B0C-A978-BCFF469B8061>>

Download the update

- * Microsoft Windows XP 64-Bit Edition Version 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=16A52196-0BD0-4355-9F29-2B26CB0961AF>>

Download the update

- * Microsoft Windows Server 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=CBCCADF6-449A-4D74-937D-4087A6E6C1C2>>

Download the update

- * Microsoft Windows Server 2003 64-Bit Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=16A52196-0BD0-4355-9F29-2B26CB0961AF>>

Download the update

- * Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (Me) Review the FAQ section of this bulletin for details about these operating systems.

Non-Affected Software:

- * Microsoft Windows XP Service Pack 2

CVE Information:

Cursor and Icon Format Handling Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1049>>

CAN-2004-1049

Windows Kernel Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1305>>

CAN-2004-1305

Cursor and Icon Format Handling Vulnerability:

A remote code execution vulnerability exists in the way that cursor, animated cursor, and icon formats are handled. An attacker could try to exploit the vulnerability by constructing a malicious cursor or icon file that could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Mitigating Factors:

- * In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability. An attacker could also attempt to compromise a Web site to have it serve up a Web page with malicious content attempting to exploit this vulnerability. An attacker would have no way to force users to visit a Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site or a site compromised by the attacker.

- * By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML

e-mail messages in the Restricted sites zone. Additionally, Outlook 2000 opens HTML e-mail messages in the Restricted sites zone if the Outlook E-mail Security Update has been installed. Outlook Express 5.5 Service Pack 2 opens HTML e-mail messages in the Restricted sites zone if Microsoft Security Bulletin

<<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 has been installed. The Restricted sites zone helps reduce attacks that could attempt to exploit this vulnerability.

* The risk of attack from the HTML e-mail vector can be significantly reduced if you meet all the following conditions:

* Apply the update that is included with Microsoft Security Bulletin <<http://go.microsoft.com/fwlink?linkid=19873>> MS03-040 or a later Cumulative Security Update for Internet Explorer.

* Use Internet Explorer 6 or later.

* Use the Microsoft <<http://go.microsoft.com/fwlink/?LinkId=33334>> Outlook E-mail Security Update, use Microsoft Outlook Express 6 or later, or use Microsoft Outlook 2000 Service Pack 2 or later in its default configuration.

* Microsoft Windows XP Service Pack 2 is not affected by this vulnerability.

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 below.

Install the Outlook E-mail Security Update if you are using Outlook 2000 SP1 or earlier.

By default, Outlook Express 6, Outlook 2002 and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 2000 opens HTML e-mail messages in the Restricted sites zone if the <<http://go.microsoft.com/fwlink/?LinkId=33334>> Outlook E-mail Security Update has been installed.

Outlook Express 5.5 Service Pack 2 opens HTML e-mail messages in the Restricted sites zone if Microsoft Security Bulletin <<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 has been installed. Customers who use any of these products could be at a reduced risk from an e-mail-borne attack that tries to exploit this vulnerability unless the user clicks a malicious link in the e-mail message.

Read e-mail messages in plain text format if you are using Outlook 2002 or later, or Outlook Express 6 SP1 or later, to help protect yourself from the HTML e-mail attack vector.

Microsoft Outlook 2002 users who have applied Office XP Service Pack 1 or later and Microsoft Outlook Express 6 users who have applied Internet Explorer 6 Service Pack 1 can enable this setting and view e-mail messages that are not digitally signed or e-mail messages that are not encrypted in plain text only.

Digitally signed e-mail messages or encrypted e-mail messages are not affected by the setting and may be read in their original formats. For

Securiteam: [NT] Vulnerability in Cursor and Icon Format Handling Allows Remote Code Execution (MS05-002)

more information about enabling this setting in Outlook 2002, see <http://support.microsoft.com/kb/307594> Microsoft Knowledge Base Article 307594.

For information about this setting in Outlook Express 6, see <http://support.microsoft.com/kb/291387> Microsoft Knowledge Base Article 291387.

Impact of Workaround: E-mail messages that are viewed in plain text format will not contain pictures, specialized fonts, animations, or other rich content. In addition:

The changes are applied to the preview pane and to open messages.

Pictures become attachments so that they are not lost.

Because the message is still in Rich Text or HTML format in the store, the object model (custom code solutions) may behave unexpectedly.

What is the scope of the vulnerability?

This is a remote code execution vulnerability. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. However, user interaction is required to exploit this vulnerability. Users whose accounts are configured to have fewer privileges on the system could be less impacted than users who operate with administrative privileges.

What causes the vulnerability?

This vulnerability exists due to insufficient format validation prior to rendering cursors, animated cursors, and icons.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take complete control of the affected system.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted web page. An attacker could also create a specially-crafted email message and send it to an affected system. Upon viewing web page, preview or reading a malicious message, the attacker could cause the affected system to execute code.

What 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.

What does the update do?

The update removes the vulnerability by modifying the way that cursors, animated cursor, and icon formats are validated prior to rendering.

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

Securiteam: [NT] Vulnerability in Cursor and Icon Format Handling Allows Remote Code Execution (MS05-002)

Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CAN-2004-1049.

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

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

Does applying this security update help protect customers from the code that has been published publicly that attempts to exploit this vulnerability?

Yes. This security update addresses the vulnerability for which proof of concept code has been published publicly. The vulnerability that has been addressed has been assigned the Common Vulnerability and Exposure number CAN-2004-1049.

Windows Kernel Vulnerability:

Mitigating Factors:

- * In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability. An attacker could also attempt to compromise a Web site to have it serve up a Web page with malicious content attempting to exploit this vulnerability. An attacker would have no way to force users to visit a Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site or a site compromised by the attacker.

- * An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

- * By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 2000 opens HTML e-mail messages in the Restricted sites zone if the Outlook E-mail Security Update has been installed. Outlook Express 5.5 Service Pack 2 opens HTML e-mail messages in the Restricted sites zone if Microsoft Security Bulletin MS04-018 has been installed. The Restricted sites zone helps reduce attacks that could attempt to exploit this vulnerability.

The risk of attack from the HTML e-mail vector can be significantly reduced if you meet all the following conditions:

- * Apply the update that is included with Microsoft Security Bulletin MS03-040 or a later Cumulative Security Update for Internet Explorer.

- * Use Internet Explorer 6 or later.

- * Use the Microsoft Outlook E-mail Security Update, use Microsoft Outlook Express 6 or later, or use Microsoft Outlook 2000 Service Pack 2 or later in its default configuration.

- * Microsoft Windows XP Service Pack 2 is not affected by this vulnerability.

Securiteam: [NT] Vulnerability in Cursor and Icon Format Handling Allows Remote Code Execution (MS05-002)

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 below.

Install the Outlook E-mail Security Update if you are using Outlook 2000 SP1 or earlier.

By default, Outlook Express 6, Outlook 2002 and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 2000 opens HTML e-mail messages in the Restricted sites zone if the Outlook E-mail Security Update has been installed.

Outlook Express 5.5 Service Pack 2 opens HTML e-mail messages in the Restricted sites zone if Microsoft Security Bulletin MS04-018 has been installed. Customers who use any of these products could be at a reduced risk from an e-mail-borne attack that tries to exploit this vulnerability unless the user clicks a malicious link in the e-mail message.

Read e-mail messages in plain text format if you are using Outlook 2002 or later, or Outlook Express 6 SP1 or later, to help protect yourself from the HTML e-mail attack vector.

Microsoft Outlook 2002 users who have applied Office XP Service Pack 1 or later and Microsoft Outlook Express 6 users who have applied Internet Explorer 6 Service Pack 1 can enable this setting and view e-mail messages that are not digitally signed or e-mail messages that are not encrypted in plain text only.

Digitally signed e-mail messages or encrypted e-mail messages are not affected by the setting and may be read in their original formats. For more information about enabling this setting in Outlook 2002, see Microsoft Knowledge Base Article 307594.

For information about this setting in Outlook Express 6, see Microsoft Knowledge Base Article 291387.

Impact of Workaround: E-mail messages that are viewed in plain text format will not contain pictures, specialized fonts, animations, or other rich content. In addition:

The changes are applied to the preview pane and to open messages.

Pictures become attachments so that they are not lost.

Because the message is still in Rich Text or HTML format in the store, the object model (custom code solutions) may behave unexpectedly.

Frequently Asked Questions:

What is the scope of the vulnerability?

This is a denial of service vulnerability. An attacker who exploited this vulnerability could cause the affected system to stop responding and automatically restart. During that time, the operating system cannot respond to requests. Note that the denial of service vulnerability would not allow attackers to execute code or elevate their privileges, but it could cause the affected system to stop responding. However, user interaction is required to exploit this vulnerability.

Securiteam: [NT] Vulnerability in Cursor and Icon Format Handling Allows Remote Code Execution (MS05-002)

What causes the vulnerability?

This vulnerability exists due to insufficient format validation prior to rendering cursors, animated cursors, and icons.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the affected system to stop responding.

How could an attacker exploit the vulnerability?

An attacker could exploit the vulnerability by creating a specially crafted web page. An attacker could also create a specially-crafted email message and send it to an affected system. Upon viewing web page, preview or reading a malicious message, the attacker could cause the affected system to stop responding

What 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.

What does the update do?

The update removes the vulnerability by modifying the way that cursors, animated cursor, and icon formats are validated prior to rendering.

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

Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CAN-2004-1305.

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

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

Does applying this security update help protect customers from the code that has been published publicly that attempts to exploit this vulnerability?

Yes. This security update addresses the vulnerability for which proof of concept code has been published publicly. The vulnerability that has been addressed has been assigned the Common Vulnerability and Exposure number CAN-2004-1305.

ADDITIONAL INFORMATION

The original article can be found at:

<http://www.microsoft.com/technet/security/bulletin/MS05-002.msp>>
<http://www.microsoft.com/technet/security/bulletin/MS05-002.msp>

Securiteam: [NT] Vulnerability in Cursor and Icon Format Handling Allows Remote Code Execution (MS05-002)

=====

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.