

# [NT] Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (MS03-044)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0066.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 14:40:05 +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 Windows Help and Support Center Could Lead to System Compromise (MS03-044)  
-----

## SUMMARY

A security vulnerability exists in the Help and Support Center function which ships with Windows XP and Windows Server 2003. The affected code is also included in all other supported Windows operating systems, although no known attack vector has been identified at this time because the HCP protocol is not supported on those platforms. The vulnerability results because a file associated with the HCP protocol contains an unchecked buffer.

## DETAILS

Vulnerable Systems:

- \*Microsoft Windows Millennium Edition
- \* 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

6

- \* Microsoft Windows 2000, Service Pack 2

[NT] Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (MS03-044)

## Securiteam: [NT] Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (MS03-044)

- \* 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

### Patch Availability:

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7D6F4228-0E31-4F46-9795-5CDD566BB3B8&dis>>

Microsoft Windows Millennium Edition

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=88BCDC9A-E370-47D8-B818-4E659C7F95AE&dis>>

Microsoft Windows NT Workstation 4.0, Service Pack 6a

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=735602AC-BA6E-40D4-8A20-3441F02A25CB&dis>>

Microsoft Windows NT Server 4.0, Service Pack 6a

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=5C16FFAB-9CE7-4444-9AA5-BC6ABE3FD479&dis>>

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

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=62B23A0C-67F0-4F11-A95E-E4FB080A63C6&dis>>

Microsoft Windows 2000, Service Pack 2

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C2AB63FD-35CA-4D33-9F8C-8BF5DE2D1117&dis>>

Microsoft Windows 2000, Service Pack 3, Service Pack 4

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=84317458-0BEB-4B2C-A095-66CA09DFDAC6&dis>>

Microsoft Windows XP Gold, Service Pack 1

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=97F4868A-5E41-4657-B9FC-7EA13954B982&displ>>

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=40F25862-A815-4674-9175-E3640E3EFD49&displa>>

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

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.

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0711>>  
CAN-2003-0711

An attacker could exploit the vulnerability by constructing a URL that, when clicked on by the user, could execute code of the attacker's choice in the Local Computer security context. The URL could be hosted on a web page, or sent directly to the user in email. In the web based scenario, where a user then clicked on the URL hosted on a website, an attacker could have the ability to read or launch files already present on the local machine.

The risk of attack from the HTML email vector can be significantly reduced if the following conditions are met:

- \* You have applied the patch included with Microsoft Security bulletin <<http://www.microsoft.com/technet/security/bulletin/MS03-040.asp>> MS03-040
- \* You are using Internet Explorer 6 or later
- \* You are using the Microsoft Outlook Email Security Update or Microsoft Outlook Express 6.0 and higher, or Microsoft Outlook 2000 or higher in their default configuration.

#### Mitigating factors:

- \* The Help and Support Center function can not be started automatically in Outlook Express or Outlook if the user is running Internet Explorer 6.0 Service Pack 1.
- \* In the Web based attack scenario, the attacker would have to host a web site that contained a web page used to exploit these vulnerabilities. An attacker would have no way to force users to visit a malicious web site outside of the HTML email vector. Instead, the attacker would need to lure them there, typically by getting them to click on a link that would take them to the attacker's site.

#### 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.

- \* Deregister the HCP Protocol.

Deregistering the HCP Protocol or changing the registration will prevent an attack from being successful. The protocol can be deregistered by deleting the following key from the registry: HKEY\_CLASSES\_ROOT\HCP.

1. From the Start Menu, select Run
2. Type regedit then click OK (The registry editor program launches)
3. Expand HKEY\_CLASSES\_ROOT and highlight the HCP key
4. Right mouse click on the HCP key, and select Delete

WARNING: Using Registry Editor incorrectly can cause serious problems that may require you to reinstall Windows. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

#### Impact of Workaround:

Deregistering the HCP protocol will break all local, legitimate help links that use hcp://. For example links in the Control Panel may no longer function.

\* Install

<<http://www.microsoft.com/office/outlook/evaluation/security.asp>> Outlook Email Security Update if you are using Outlook 2000 SP1 or Earlier. The Outlook Email Security Update causes Outlook 98 and 2000 to open HTML mail in the Restricted Sites Zone by default. Outlook Express 6.0 and Outlook 2002 by default open HTML mail in the Restricted Sites Zone. Customers who use any of these products would be at a reduced risk from an e-mail borne attack that attempts to exploit this vulnerability unless the user clicks a malicious link in the email

\* If you are using Outlook 2002 or Outlook Express 6.0SP1 or higher, to help protect yourself from the HTML email attack vector, read email in plain text format.

Users of Microsoft Outlook 2002 and Outlook Express 6.0 who have applied Service Pack 1 and or higher can enable a feature to view all non-digitally-signed e-mail or non-encrypted e-mail messages in plain text only.

Digitally signed e-mail or encrypted e-mail messages are not affected by the setting and may be read in their original formats. Information on enabling this setting in Outlook 2002 can be found in the following Knowledge Base article:

<<http://support.microsoft.com/default.aspx?scid=kb:en-us:307594>>  
<http://support.microsoft.com/default.aspx?scid=kb:en-us:307594>

Information on enabling this setting in Outlook Express 6.0 can be found in the following Knowledge Base article:

<<http://support.microsoft.com/?kbid=291387>>  
<http://support.microsoft.com/?kbid=291387>

Impact of Workaround:

E-mail viewed in plain text format cannot contain pictures, specialized fonts, animations, or other rich content. In addition:

- \* The changes are applied to the preview pane and open messages.
- \* Pictures become attachments to avoid loss.
- \* Since the message is still in Rich Text or HTML format in the store, the object model (custom code solutions) may behave unexpectedly because the message is still in Rich Text or HTML format in the mail store.

Frequently Asked Questions

What's the scope of this vulnerability?

This is a buffer overrun vulnerability. An attacker who successfully exploited this vulnerability could cause code of their choice to be executed as though it originated on the local machine. Such code could provide the attacker with the ability to take any desired action on the machine, including adding, deleting or modifying data on the system or running any code of the attacker's choice.

What causes the vulnerability?

The vulnerability results because of an unchecked buffer in file associated with the HCP protocol which is owned by the Help and Support Center.

What is the Help and Support Center?

Help and Support Center (HSC) is a feature in Windows that provides help on a variety of topics. For instance, HSC enables users to learn about Windows features, download and install software updates, determine whether a particular hardware device is compatible with Windows, get assistance from Microsoft, and so forth.

Users and programs can execute URL links to Help and Support Center by using the "hcp://" prefix in a URL link instead of "http://".

What is the HCP protocol?

Similar to the HTTP protocol which is used to execute URL links to open a web browser, the HCP protocol can be used to execute URL links to open the Help and Support Center feature.

What's wrong with the HCP protocol?

There is an unchecked buffer in an associated file used by the HCP protocol. This file is used by the Help and Support Center feature and is invoked automatically when HSC is launched.

What could this vulnerability enable an attacker to do?

This vulnerability could enable an attacker to cause code of their choice to run with additional privileges on the system. This could allow the attacker to add, delete or modify data on the system, or take any other action of the attacker's choice.

How could an attacker exploit this vulnerability?

The attacker would need to construct a web page that launched a specially crafted URL. The attack could then proceed via either of two vectors. In the first, the attacker could host the web page on a web site; when a user visited the site, the web page would attempt to launch the URL and exploit the vulnerability. In the second, the attacker could send the web page as an HTML mail. Upon being opened by the recipient, the web page could attempt to invoke the function and exploit the vulnerability.

Why is this vulnerability listed only as "Low" on all systems prior to Windows XP?

The specific file which actually contains the vulnerable code is present on all versions of Microsoft Windows, but the Help and Support Center functionality, which is required to exploit the vulnerability, is not available or supported on platforms prior to Windows XP.

Is there anything that helps mitigate the risk of an HTML email attack?

The risk of attack from the HTML email vector can be significantly reduced if the following conditions are met:

- \* You have applied the patch included with Microsoft Security bulletin <http://www.microsoft.com/technet/security/bulletin/MS03-040.asp> MS03-040
- \* You are using Internet Explorer 6 or later
- \* You are using the Microsoft Outlook Email Security Update or Microsoft Outlook Express 6.0 and higher, or Microsoft Outlook 2000 or higher in their default configuration.

Securiteam: [NT] Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (MS03-044)

What does the patch do?

The patch addresses the vulnerability by correcting the unchecked buffer in the file associated with the HCP protocol.

Microsoft thanks the following for working with us to protect customers:  
David Litchfield of <<http://www.nextgenss.com>> Next Generation Security Software Ltd. for reporting the issue in MS03-044.

ADDITIONAL INFORMATION

The original article can be found at:  
<<http://www.microsoft.com/technet/security/bulletin/MS03-044.asp>>  
<http://www.microsoft.com/technet/security/bulletin/MS03-044.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.