

# [NT] Microsoft PCHealth Buffer Overflow Vulnerability (Technical Details)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0079.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 10/19/03

To: list@securiteam.com

Date: 19 Oct 2003 14:34:51 +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>

-----

Microsoft PCHealth Buffer Overflow Vulnerability (Technical Details)

---

## SUMMARY

Microsoft Windows 2003 Server and Windows XP provide a support and troubleshooting facility called PCHealth. PCHealth provides users with information on how to deal with any problems they may experience. PCHealth contains search functionality allowing users to search using keywords. The Search engine runs as a system service and is vulnerable to an exploitable stack based buffer overflow condition.

We reported on this issue in our previous article:

<<http://www.securiteam.com/windowsntfocus/6M00F1P8KU.html>> Vulnerability in Authenticode Verification Could Allow Remote Code Execution (MS03-041).

## DETAILS

The PCHealth system can be launched in several different ways. It can be launched via an HTML document rendered in Internet Explorer or Outlook using the HCP protocol or via DCOM. This presents remote attackers with several vectors to launch an attack; however, the latter requires administrative privileges already so is not a likely attack vector. It is listed for the sake of completeness. Local attackers can, of course, also

## Securiteam: [NT] Microsoft PCHealth Buffer Overflow Vulnerability (Technical Details)

exploit this vulnerability to gain control of the system. The vulnerability is a stack based buffer overflow triggered by an overly long query and exists in the Help Service (helpsvc.exe) which is started by svchost.exe. As the instance of svchost that runs the Help and Support service is also responsible for running other services that require SYSTEM privileges it is not possible to help mitigate the risk by setting a low privileged account to run this service. In the absence of a patch it is suggested that the Help and Support service be disabled until the patch can be applied.

Notes on Windows 2003:

Despite the stack protection built into Windows 2003 (through Visual C++ NET), this overflow can still be exploited. (Please read the following paper for more details –

<<http://www.nextgenss.com/papers/defeating-w2k3-stack-protection.pdf>>  
<http://www.nextgenss.com/papers/defeating-w2k3-stack-protection.pdf>)

That said, by default, the security settings of Internet Explorer and Outlook Express on Windows 2003 mitigate the risk these systems are exposed to via the HTML vector. Local low privileged attackers can still exploit this to gain control but best practices dictate that only administrators should be allowed to log on to servers. Provided these precautions have been followed (or left in place) then the risk posed to Windows 2003 Servers is reduced somewhat. That said NGSS advises that the patch still be applied once proper testing of the patch has been done.

Fix Information:

Microsoft has supplied a patch for this problem that can be downloaded from:

<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-041.asp>>  
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-041.asp>

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:nisr@nextgenss.com>>  
NGSSoftware Insight Security Research.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.