

Microsoft PCHealth 2003/XP Buffer Overflow (#NISR15102003)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-10/0179.html>

From: NGSSoftware Insight Security Research (*nistr_at_nextgenss.com*)

Date: 10/16/03

To: <bugtraq@securityfocus.com>, <ntbugtraq@listserv.ntbugtraq.com>, <vulnwatch@vulnwatch.org>

Date: Thu, 16 Oct 2003 12:21:12 +0100

NGSSoftware Insight Security Research Advisory

Name: Microsoft PCHealth Buffer Overflow Vulnerability

Systems Affected: Windows 2003 and XP

Severity: Critical Risk

Vendor URL: <http://www.microsoft.com/>

Author: David Litchfield [david@ngssoftware.com]

Date Vendor Notified: 23rd July 2003

Date of Public Advisory: 15th October 2003

Advisory number: #NISR15102003

Advisory URL: <http://www.ngssoftware.com/advisories/ms-pchealth.txt>

Description

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.

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 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

SecurityFocus Bugtraq: Microsoft PCHealth 2003/XP Buffer Overflow (#NISR15102003)

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>)

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 have 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>

About NGSSoftware

NGSSoftware design, research and develop intelligent, advanced application security assessment scanners. Based in the United Kingdom, NGSSoftware have offices in the South of London and the East Coast of Scotland. NGSSoftware's sister company NGSConsulting, offers best of breed security consulting services, specialising in application, host and network security assessments.

<http://www.ngssoftware.com/>

Telephone +44 208 401 0070

Fax +44 208 401 0076

enquiries@ngssoftware.com