

US-CERT Technical Cyber Security Alert TA05-012B -- Microsoft Windows HTML Help ActiveX Control Cross-Domain Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Cert/2005-01/0002.html>

From: CERT Advisory (cert-advisory_at_cert.org)

Date: 01/13/05

Date: Wed, 12 Jan 2005 22:45:22 -0500

To: cert-advisory@cert.org

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Technical Cyber Security Alert TA05-012B

Microsoft Windows HTML Help ActiveX Control Cross-Domain Vulnerability

Original release date: January 12, 2005

Last revised: --

Source: US-CERT

Systems Affected

- * Windows 98, Me, 2000, XP, and Server 2003
- * Internet Explorer 5.x and 6.x
- * Other Windows programs that use MSHTML

Overview

The Microsoft Windows HTML Help ActiveX control contains a cross-domain vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary commands or code with the privileges of the user running the control. The HTML Help control can be instantiated by an HTML document loaded in Internet Explorer or any other program that uses MSHTML.

I. Description

The Microsoft Windows HTML Help ActiveX control (hhctrl.ocx) does not properly determine the source of windows opened by the Related Topics command. If an HTML Help control opens a Related Topics

window in one domain, and a second control opens a Related Topics window using the same window name in a different domain, content from the second window is considered to be in the domain of the first window. This cross-domain vulnerability allows an attacker in one domain to read or modify content or execute script in a different domain, including the Local Machine Zone.

An attacker could exploit this vulnerability against Internet Explorer (IE) using a specially crafted web site. Other programs that use MSHTML, including Outlook and Outlook Express, could also act as attack vectors.

This vulnerability has been assigned CVE CAN-2004-1043 and is described in further detail in VU#972415.

II. Impact

By convincing a user to view a specially crafted HTML document (e.g., a web page or an HTML email message), an attacker could execute arbitrary code or commands with the privileges of the user. The attacker could also read or modify data in other web sites.

Reports indicate that this vulnerability is being exploited by malicious code referred to as Phel.

III. Solution

Install an update

Install the appropriate update according to Microsoft Security Bulletin MS05-001. Note that the update may adversely affect the HTML Help system as described in Microsoft Knowledge Base articles 892641 and 892675.

Workarounds

A number of workarounds are described in MS05-001 and VU#972415.

Appendix A. References

- * Vulnerability Note VU#972415 –
<<http://www.kb.cert.org/vuls/id/972415>>
- * Microsoft Security Bulletin MS05-001 –
<<http://www.microsoft.com/technet/security/bulletin/ms05-001.msp>>
- * HTML Help files do not work correctly after you uninstall security update 890175 (MS05-001) –
<<http://support.microsoft.com/kb/892641>>

* You cannot access HTML Help functionality on some Web sites after installing security update MS05-001 –
<<http://support.microsoft.com/kb/892675>>

* Reusing MSHTML –
<<http://msdn.microsoft.com/workshop/browser/hosting/hosting.asp>>

* HTML Help ActiveX Control Overview –
<<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/htmlhelp/html/vsconocxov.asp>>

* Related Topics –
<<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/htmlhelp/html/vsconocxrelatedtopics.asp>>

* About the Browser (Internet Explorer – WebBrowser) –
<<http://msdn.microsoft.com/workshop/browser/overview/Overview.asp>>

* CVE CAN-2004-1043 –
<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1043>>

Feedback can be directed to the author: Art Manion.

Send mail to <cert@cert.org>.

Please include the subject line "TA05-012B Feedback VU#972415".

Copyright 2005 Carnegie Mellon University.

Terms of use: <<http://www.us-cert.gov/legal.html>>

The most recent version of this document can be found at:

<<http://www.us-cert.gov/cas/techalerts/TA05-012B.html>>

Revision History

January 12, 2005: Initial release

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.1 (GNU/Linux)

iQEVAwUBQeXt5hhoSezw4YfQAQKGDAf+Lb6gU16gDtrWunNwgcTAEoNkTStKIDzX
zvPjKjEfvuM58EcRDzaJnqeinvuKO37c3OMwuZ/5MGZy6rIb45auD3hG3uQSDNWj
7tlADBoU24Bqj5Hcskz3ePAkRxI+Ex06di4N3F/qUVnDBbyZi+oTmIPBabLpcnhV
9yy4W5ihHLxfAOEDUWVZYb2xqdGLh9CP1G9TRNH3cjCxAHf60WV/QDbpuX8JO4dW
vdsgUfDOxW1+6g0l2BvIqUG2AfPorsBWZ1VhhCTrhyKn0is2rqG17YbZ7lWDKLRp
M8Fm4ynpVLexcN2qC3VxZI0dFn3yXRy1q1946DRlX6VqGuA12ZlWyA==
=yHDO
-----END PGP SIGNATURE-----