

[NT] Vulnerability in Help and Support Center Remote Code Execution (MS04-015)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-05/0049.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/12/04

To: list@securiteam.com

Date: 12 May 2004 19:03:19 +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>

Vulnerability in Help and Support Center Remote Code Execution (MS04-015)

SUMMARY

A remote code execution vulnerability exists in the Help and Support Center because of the way that it handles HCP URL validation. An attacker could exploit the vulnerability by constructing a malicious HCP URL that could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

DETAILS

Vulnerable Systems:

- * Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- * Microsoft Windows XP 64-Bit Edition Service Pack 1
- * Microsoft Windows XP 64-Bit Edition Version 2003
- * Microsoft Windows Server 2003
- * Microsoft Windows Server 2003 64-Bit Edition

Immune Systems:

Securiteam: [NT] Vulnerability in Help and Support Center Remote Code Execution (MS04-015)

- * 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
- * Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000 Service Pack 3, Microsoft Windows 2000 Service Pack 4
- * Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

Patch Availability:

- * Microsoft Windows XP and Microsoft Windows XP Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=563F65A3-D793-47B4-A607-948CAA5B3454&dis>

Download the update

- * Microsoft Windows XP 64-Bit Edition Service Pack 1 –

<