

[VulnWatch] Buffer Overflow in IE/Outlook HTML Help

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-10/0010.html>

From: NGS Insight Security Research (nisr@nextgenss.com)

Date: 10/03/02

From: "NGS Insight Security Research" <nisr@nextgenss.com>

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

Date: Thu, 3 Oct 2002 15:21:10 +0100

NGSSoftware Insight Security Research Advisory

Name: Windows Help System Buffer Overflow

Systems: Windows XP,2000,NT,ME and 98

Severity: High Risk

Category: Buffer Overflow Vulnerability

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

Author: David Litchfield (david@ngssoftware.com)

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

Date: 2nd October 2002

Advisory number: #NISR02102002

Introduction

The Windows Help system includes an ActiveX control known as the HTML Help Control, hhctrl.ocx. The "Alink" function of this control is vulnerable to a buffer overflow that can be exploited to gain control of the user's machine.

Details

By providing an overly long parameter to the vulnerable function an internal buffer is overflowed and program control structures can be overwritten allowing an attacker to remotely gain control of their victims PC. This could be done by enticing the victim to a website that contained a webpage that exploits the vulnerability or by sending the victim an HTML mail. When opened in Outlook the overflow will be triggered.

Fix Information

Microsoft have produced a patch which is available from their web site. More details are available from