

Buffer overflow in MSIE gopher code (fwd)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-06/0002.html>

From: Jouko Pynnonen (jouko@SOLUTIONS.FI)

Date: 06/06/02

Date: Thu, 6 Jun 2002 17:01:57 +0300
From: Jouko Pynnonen <jouko@SOLUTIONS.FI>
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

----- Forwarded message -----

Date: Tue, 4 Jun 2002 16:07:34 +0300 (EEST)
From: Jouko Pynnonen <jouko@solutions.fi>
To: bugtraq@securityfocus.com
Subject: Buffer overflow in MSIE gopher code

OVERVIEW

=====

Gopher is a protocol developed at the University of Minnesota in the early 1990's. Gopher servers offer hierarchically organized directories and files. These form a "gopherspace" which can be thought of as the predecessor of the World Wide Web. Gopher was mostly abandoned soon after HTTP and the World Wide Web started gaining popularity.

Microsoft Internet Explorer has a built-in gopher client. Gopher pages can be accessed via URLs starting with "gopher://". The part of code in IE which parses gopher replies contains an exploitable buffer overflow bug. A malicious server may be used to run arbitrary code on an IE user's system.

DETAILS

=====

When the overflow is triggered, a fixed sized buffer in stack gets overwritten with data from the gopher server. This data can contain most octets from 0 to 255 (also nulls) which makes it particularly easy to inject a working shellcode in it. This is a traditional, trivially exploitable buffer overflow. A test exploit has been successfully used to run arbitrary code without user intervention with various IE versions and systems including IE 5.5 and 6.0.

The attack can be launched via a web page or an HTML mail message which redirect the user to a malicious gopher server when the victim views them. The server can be very minimal, ie. a program that can listen on a TCP port and write a block of data; a fully operational gopher server isn't

NT-Bugtraq: Buffer overflow in MSIE gopher code (fwd)

necessary in order to carry out the attack.

The exploiter could do anything that a regular user could do on the system: retrieve, install, or remove files, upload and run programs, etc.

Full technical details aren't disclosed at this time to prevent exploitation.

WORKAROUND

=====

Internet Explorer users can protect themselves from the flaw by disabling the gopher protocol. Barely any gopher servers exist on the Internet today, so this is unlikely to cause problems. If needed, a gopher client or some other web browser can be used to access the gopherspace.

An easy way to disable processing and displaying gopher pages is to define a non-functional gopher proxy in Internet Options. Select Tools -> Internet options -> Connections. Click on "LAN settings". Check "Use a proxy server for your LAN". Click on "Advanced...". Here you can define proxy servers to be used with different protocols. Go to the Gopher text field and enter "localhost", and "1" in the port text field. This will stop Internet Explorer from fetching any gopher documents.

After installing the patch from Microsoft you can remove these gopher proxy settings (or restore them to values they had before).

For more information and a vulnerability test see

<http://www.solutions.fi>

VENDOR STATUS

=====

Microsoft was contacted on May 20th. At the moment of writing this advisory, Microsoft has started designing and coding a fix, but hasn't given any approximation of when it would be released. The patch will be available at

<http://www.microsoft.com/technet/security/current.asp>

when it is completed.

--

Jouko Pynnonen
jouko@solutions.fi

Online Solutions Ltd
<http://www.solutions.fi>

Secure your Linux -
<http://www.secmod.com>

-
- **Previous message:** [Russ: "Re: Self-Executing HTML: Internet Explorer 5.5 and 6.0"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)