Nessus Report

Report

24/Feb/2012:17:48:13 GMT

Table Of Contents

Vulnerabilities By Host

192.168.1.205

Scan Information

Start time:	Tue Feb 14 13:24:57 2012
End time:	Tue Feb 14 13:26:55 2012

Host Information

DNS Name:	WINDOWS2000
Netbios Name:	WINDOWS2000
IP:	192.168.1.205
MAC Address:	00:0c:29:f7:55:ea
OS:	Microsoft Windows 2000 Professional (English)

Results Summary

Critical	High	Medium	Low	Info	Total
31	150	30	2	0	213

Results Details

445/tcp

15456 - MS04-031: Vulnerability in NetDDE Could Allow Code Execution (841533)

Description

The remote version of Windows is affected by a vulnerability in Network Dynamic Data Exchange (NetDDE).
To exploit this flaw, NetDDE would have to be running and an attacker with a specific knowledge of the vulnerability would need to send a malformed NetDDE message to the remote host to overrun a given buffer.
A public exploit is available to exploit this vulnerability.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	11372
CVE	CVE-2004-0206
XREF	MSFT:MS04-031
XREF	OSVDB:10689

Exploitable with

CANVAS (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Netdde.exe has not been patched
    Remote version : 5.0.2195.6601
    Should be : 5.0.2195.6952
```

12052 - MS04-007: ASN.1 parsing vulnerability (828028)

Description

The remote Windows host has a ASN.1 library that is vulnerable to a flaw that could allow an attacker to execute arbitrary code on this host.
To exploit this flaw, an attacker would need to send a specially crafted ASN.1 encoded packet (either an IPsec session negotiation, or an HTTPS request) with improperly advertised lengths.
A public code is available to exploit this flaw.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	13300
BID	9635
BID	9633
CVE	CVE-2003-0818
XREF	MSFT:MS04-007
XREF	IAVA:2004-A-0001
XREF	OSVDB:3902

Exploitable with

CANVAS (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Msasn1.dll has not been patched
    Remote version : 5.0.2195.6666
    Should be : 5.0.2195.6823
```

39344 - MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)

Description

The version of the Print Spooler service on the remote Windows host is affected by one or more of the following vulnerabilities :
- A buffer overflow vulnerability could allow an unauthenticated, remote attacker to execute arbitrary code with SYSTEM privileges. (CVE-2009-0228)
- Using a specially crafted separator page, a local user can read or print any file on the affected system. (CVE-2009-0229)
- Using a specially crafted RPC message, a user who has the 'Manage Printer' privilege can have the spooler load an arbitrary DLL and thereby execute arbitrary code with elevated privileges. (CVE-2009-0230)

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	35209

BID	35208
BID	35206
CVE	CVE-2009-0230
CVE	CVE-2009-0229
CVE	CVE-2009-0228
XREF	MSFT:MS09-022
XREF	OSVDB:54934
XREF	OSVDB:54933
XREF	OSVDB:54932
XREF	CWE:264

Exploitable with

CANVAS (true)Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\Localspl.dll has not been patched
    Remote version : 5.0.2195.6714
    Should be : 5.0.2195.7296
```

39348 - MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (970238)

Description

The RPC Marshalling Engine installed on the remote Windows host does not update its internal state appropriately, which could lead to a pointer being read from an incorrect location. A remote attacker may be able to leverage this issue to execute arbitrary code on the affected host and take complete control of it.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	35219
CVE	CVE-2009-0568
XREF	MSFT:MS09-026
XREF	OSVDB:54936
XREF	CWE:264

Ports

tcp/445

```
- C:\WINNT\system32\Rpcrt4.dll has not been patched
    Remote version : 5.0.2195.6701
    Should be : 5.0.2195.7281
```

12205 - MS04-011: Microsoft Hotfix (credentialed check) (835732)

Description

The remote host is missing a critical Microsoft Windows Security Update (835732).
This update fixes various flaws that could allow an attacker to execute arbitrary code on the remote host.
A series of worms (Sasser) are known to exploit this vulnerability in the wild.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	10125
BID	10124
BID	10122
BID	10119
BID	10117
BID	10113
BID	10111
CVE	CVE-2004-0121
CVE	CVE-2004-0119
CVE	CVE-2004-0118
CVE	CVE-2004-0117
CVE	CVE-2003-0910
CVE	CVE-2003-0909
CVE	CVE-2003-0908
CVE	CVE-2003-0907
CVE	CVE-2003-0906
CVE	CVE-2003-0806
CVE	CVE-2003-0719
CVE	CVE-2003-0663
CVE	CVE-2003-0533
XREF	MSFT:MS04-011
XREF	IAVA:2004-A-0006
XREF	OSVDB:5259
XREF	OSVDB:5258

XREF	OSVDB:5257
XREF	OSVDB:5256
XREF	OSVDB:5255
XREF	OSVDB:5254
XREF	OSVDB:5253
XREF	OSVDB:5252
XREF	OSVDB:5251
XREF	OSVDB:5250
XREF	OSVDB:5249
XREF	OSVDB:5248
XREF	OSVDB:4168

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Lsasrv.dll has not been patched
    Remote version : 5.0.2195.6695
    Should be : 5.0.2195.6902
```

19402 - MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)

Description

The remote version of Windows contains a flaw in the function PNP_QueryResConfList() in the Plug and Play service that could allow an attacker to execute arbitrary code on the remote host with the SYSTEM privileges.
A series of worms (Zotob) are known to exploit this vulnerability in the wild.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	14513
CVE	CVE-2005-1983
XREF	MSFT:MS05-039
XREF	IAVA:2005-A-0025
XREF	OSVDB:18605

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\umpnpmgr.dll has not been patched
    Remote version : 5.0.2182.1
    Should be : 5.0.2195.7057
```

43063 - MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)

Description

The remote Windows host has the following vulnerabilities in the Internet Authentication Service :
- There is a memory corruption vulnerability in the PEAP authentication implementation. A remote, unauthenticated attacker could exploit this to execute arbitrary code as SYSTEM. (CVE-2009-2505)
- Sending a specially crafted MS-CHAP v2 authentication request could allow a remote attacker to obtain the privileges of a specific, authorized user. (CVE-2009-3677)

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	37198
BID	37197
CVE	CVE-2009-3677
CVE	CVE-2009-2505
XREF	CWE:94
XREF	CWE:255
XREF	MSFT:MS09-071
XREF	IAVA:2009-A-0126
XREF	OSVDB:60833
XREF	OSVDB:60832

Ports

tcp/445

```
- C:\WINNT\system32\Rastls.dll has not been patched
    Remote version : 5.0.2195.6680
    Should be : 5.0.2195.7344
```

18483 - MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422)

Description

The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that could allow an attacker to execute arbitrary code on the remote host.
An attacker does not need to be authenticated to exploit this flaw.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	13942
CVE	CVE-2005-1206
XREF	MSFT:MS05-027
XREF	OSVDB:17308

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\drivers\Srv.sys has not been patched
    Remote version : 5.0.2195.6699
    Should be : 5.0.2195.7044
```

11790 - MS03-026 / MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (823980 / 824146)

Description

The remote host is running a version of Windows affected by several vulnerabilities in its RPC interface and RPCSS Service, that could allow an attacker to execute arbitrary code and gain SYSTEM privileges.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8460
BID	8459
BID	8458
BID	8205
CVE	CVE-2003-0605
CVE	CVE-2003-0528
CVE	CVE-2003-0715
CVE	CVE-2003-0352
XREF	MSFT:MS03-039
XREF	MSFT:MS03-026
XREF	IAVA:2003-A-0012
XREF	IAVA:2003-A-0011
XREF	OSVDB:2535
XREF	OSVDB:2100
XREF	OSVDB:11797

XREF	OSVDB:11460

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Rpcrt4.dll has not been patched
    Remote version : 5.0.2195.6701
    Should be : 5.0.2195.6753
```

11921 - MS03-049: Buffer Overflow in the Workstation Service (828749)

Description

The remote version of Windows contains a flaw in the function NetpValidateName() in the WorkStation service that could allow an attacker to execute arbitrary code on the remote host with the SYSTEM privileges.
A series of worms (Welchia, Spybot, ...) are known to exploit this vulnerability in the wild.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	9011
CVE	CVE-2003-0812
XREF	MSFT:MS03-049
XREF	IAVA:2003-A-0018
XREF	CERT:CA-2003-28
XREF	OSVDB:11461

Exploitable with

CANVAS (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\wkssvc.dll has not been patched
    Remote version : 5.0.2195.6692
    Should be : 5.0.2195.6862
```

22182 - MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883)

Description

The remote host is vulnerable to a buffer overrun in the 'Server' service that could allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.7 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	19409
CVE	CVE-2006-3439
XREF	MSFT:MS06-040
XREF	IAVA:2006-A-0036
XREF	OSVDB:27845

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Netapi32.dll has not been patched
    Remote version : 5.0.2195.6601
    Should be : 5.0.2195.7105
```

35361 - MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)

Description

The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	33122
BID	33121
BID	31179
CVE	CVE-2008-4114
CVE	CVE-2008-4835
CVE	CVE-2008-4834
XREF	CWE:399
XREF	MSFT:MS09-001
XREF	IAVA:2009-A-0002
XREF	OSVDB:52692
XREF	OSVDB:52691
XREF	OSVDB:48153

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\drivers\Srv.sys has not been patched
    Remote version : 5.0.2195.6699
    Should be : 5.0.2195.7222
```

29893 - MS08-001: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (941644)

Description

The remote version of Windows contains a version of the TCP/IP protocol that does not properly parse IGMPv3, MLDv2 and ICMP structure.
An attacker may exploit these flaws to execute code on the remote host.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	27139
BID	27100
CVE	CVE-2007-0069
CVE	CVE-2007-0066
XREF	MSFT:MS08-001
XREF	OSVDB:40070
XREF	OSVDB:40069

Exploitable with

CANVAS (true)Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\drivers\Tcpip.sys has not been patched
    Remote version : 5.0.2195.6706
    Should be : 5.0.2195.7147
```

12206 - MS04-012: Microsoft Hotfix (credentialed check) (828741)

Description

The remote host has multiple bugs in its RPC/DCOM implementation (828741).
An attacker could exploit one of these flaws to execute arbitrary code on the remote system.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8811

BID	10127
BID	10123
BID	10121
CVE	CVE-2004-0124
CVE	CVE-2003-0807
CVE	CVE-2004-0116
CVE	CVE-2003-0813
XREF	MSFT:MS04-012
XREF	IAVA:2004-A-0005
XREF	OSVDB:5247
XREF	OSVDB:5246
XREF	OSVDB:5245
XREF	OSVDB:2670

Ports
tcp/445

```
- C:\WINNT\system32\Rpcrt4.dll has not been patched
    Remote version : 5.0.2195.6701
    Should be : 5.0.2195.6904
```

44422 - MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)

Description

The remote host is affected by several vulnerabilities in the SMB server that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	38085
BID	38054
BID	38051
BID	38049
CVE	CVE-2010-0231
CVE	CVE-2010-0022
CVE	CVE-2010-0021
CVE	CVE-2010-0020

XREF	CWE:264
XREF	CWE:310
XREF	MSFT:MS10-012
XREF	IAVA:2010-A-0031
XREF	OSVDB:62256
XREF	OSVDB:62255
XREF	OSVDB:62254
XREF	OSVDB:62253

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\drivers\Srv.sys has not been patched
    Remote version : 5.0.2195.6699
    Should be : 5.0.2195.7365
```

22183 - MS06-041: Vulnerability in DNS Resolution Could Allow Remote Code Execution (920683)

Description

The remote host is vulnerable to a buffer overrun in the DNS client service, which could allow an attacker to execute arbitrary code on the remote host with SYSTEM privileges.
To exploit this vulnerability, an attacker would need to set up a rogue DNS server to reply to the client with a specially crafted packet.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	19404
BID	19319
CVE	CVE-2006-3441
CVE	CVE-2006-3440
XREF	MSFT:MS06-041
XREF	OSVDB:27844
XREF	OSVDB:27843

Ports

tcp/445

```
- C:\WINNT\system32\Dnsapi.dll has not been patched
    Remote version : 5.0.2195.6680
    Should be : 5.0.2195.7100
```

11888 - MS03-043: Buffer Overrun in Messenger Service (828035)

Description

The remote version of Windows contains a Heap Overflow in the Messenger service that could allow an attacker to execute arbitrary code on the remote host with the SYSTEM privileges.
A series of worms (Gaobot, Agobot, ...) are known to exploit this vulnerability in the wild.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8826
CVE	CVE-2003-0717
XREF	MSFT:MS03-043
XREF	IAVA:2003-A-0017
XREF	OSVDB:10936

Exploitable with

CANVAS (true)

Ports

tcp/445

```
- C:\WINNT\system32\Msgsvc.dll has not been patched
    Remote version : 5.0.2195.6656
    Should be : 5.0.2195.6861
```

21692 - MS06-030: Vulnerability in Server Message Block Could Allow Elevation of Privilege (914389)

Description

The remote version of Windows contains a version of SMB (Server Message Block) protocol that is affected by several vulnerabilities.
An attacker may exploit these flaws to elevate his privileges and gain control of the remote host.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	18357
BID	18356
CVE	CVE-2006-2374
CVE	CVE-2006-2373
XREF	MSFT:MS06-030
XREF	OSVDB:26440

XREF	OSVDB:26439

Ports
tcp/445

```
- C:\WINNT\system32\drivers\Mrxsmb.sys has not been patched
    Remote version : 5.0.2195.6713
    Should be : 5.0.2195.7097
```

19406 - MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (896423)

Description
The remote host contains a version of the Print Spooler service that is vulnerable to a security flaw that could allow an attacker to execute code on the remote host or crash the spooler service.
An attacker can execute code on the remote host with a NULL session against :
- Windows 2000
An attacker can crash the remote service with a NULL session against :
- Windows 2000
- Windows XP SP1
An attacker needs valid credentials to crash the service against :
- Windows 2003
- Windows XP SP2

Risk Factor
Critical

CVSS Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score
8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References
BID	14514
CVE	CVE-2005-1984
XREF	MSFT:MS05-043
XREF	OSVDB:18607

Exploitable with
CANVAS (true)Core Impact (true)

Ports
tcp/445

```
- C:\WINNT\system32\Spoolsv.exe has not been patched
    Remote version : 5.0.2195.6659
    Should be : 5.0.2195.7054
```

23646 - MS06-070: Vulnerability in Workstation Service Could Allow Remote Code Execution (924270)

Description
The remote host is vulnerable to a buffer overrun in the 'workstation' service that could allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Risk Factor
Critical

CVSS Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score
8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	20985
CVE	CVE-2006-4691
XREF	MSFT:MS06-070
XREF	IAVA:2006-A-0054
XREF	OSVDB:30263

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Netapi32.dll has not been patched
    Remote version : 5.0.2195.6601
    Should be : 5.0.2195.7108
```

34476 - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution (958644)

Description

The remote host is vulnerable to a buffer overrun in the 'Server' service that could allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.7 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	31874
CVE	CVE-2008-4250
XREF	CWE:94
XREF	MSFT:MS08-067
XREF	IAVA:2008-A-0081
XREF	OSVDB:49243

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Netapi32.dll has not been patched
    Remote version : 5.0.2195.6601
    Should be : 5.0.2195.7203
```

20004 - MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)

Description

The remote version of Windows contains a version of MSDTC and COM+ that is affected by several remote code execution, local privilege escalation and denial of service vulnerabilities.

An attacker may exploit these flaws to obtain the complete control of the remote host.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	15056
BID	15057
BID	15058
BID	15059
CVE	CVE-2005-1980
CVE	CVE-2005-1979
CVE	CVE-2005-1978
CVE	CVE-2005-2119
XREF	MSFT:MS05-051
XREF	IAVA:2005-A-0030
XREF	OSVDB:19904
XREF	OSVDB:19903
XREF	OSVDB:19902
XREF	OSVDB:18828

Ports

tcp/445

```
- C:\WINNT\system32\ole32.dll has not been patched
    Remote version : 5.0.2195.6692
    Should be : 5.0.2195.7059
```

19999 - MS05-046: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589)

Description

The remote host contains a version of the Client Service for NetWare that is vulnerable to a buffer overflow. An attacker could exploit this flaw by connecting to the NetWare RPC service (possibly over IP) and trigger the overflow by sending a malformed RPC request.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	15066
CVE	CVE-2005-1985
XREF	MSFT:MS05-046
XREF	OSVDB:19922

Exploitable with

CANVAS (true)Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\nwwks.dll has not been patched
    Remote version : 5.0.2195.6602
    Should be : 5.0.2195.7065
```

24340 - MS07-016: Cumulative Security Update for Internet Explorer (928090)

Description

The remote host is missing the IE cumulative security update 92808.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	22504
BID	22489
BID	22486
CVE	CVE-2007-0217
CVE	CVE-2007-0219
CVE	CVE-2006-4697
XREF	MSFT:MS07-016
XREF	IAVA:2007-A-0018
XREF	OSVDB:31895
XREF	OSVDB:31894
XREF	OSVDB:31893
XREF	OSVDB:31892
XREF	OSVDB:31891

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
```

```
Remote version : 5.0.3700.6699
Should be : 5.0.3849.500
```

11808 - MS03-026: Microsoft RPC Interface Buffer Overrun (823980)

Description

The remote version of Windows contains a flaw in the function RemoteActivation() in its RPC interface that could allow an attacker to execute arbitrary code on the remote host with the SYSTEM privileges.
A series of worms (Blaster) are known to exploit this vulnerability in the wild.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8205
CVE	CVE-2003-0352
XREF	MSFT:MS03-026
XREF	IAVA:2003-A-0011
XREF	OSVDB:2100

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

18502 - MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)

Description

The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that may allow an attacker to execute arbitrary code on the remote host.
An attacker does not need to be authenticated to exploit this flaw.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	13942
CVE	CVE-2005-1206
XREF	MSFT:MS05-027
XREF	OSVDB:17308

Exploitable with

Core Impact (true)

Ports

tcp/445

19407 - MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check)

Description

The remote host contains a version of the Print Spooler service that may allow an attacker to execute code on the remote host or crash the spooler service.
An attacker can execute code on the remote host with a NULL session against :
- Windows 2000
An attacker can crash the remote service with a NULL session against :
- Windows 2000
- Windows XP SP1
An attacker needs valid credentials to crash the service against :
- Windows 2003
- Windows XP SP2

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	14514
CVE	CVE-2005-1984
XREF	MSFT:MS05-043
XREF	OSVDB:18607

Exploitable with

CANVAS (true)Core Impact (true)

Ports

tcp/445

11835 - MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)

Description

The remote host is running a version of Windows that has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges.
An attacker or a worm could use it to gain the control of this host.
Note that this is NOT the same bug as the one described in MS03-026, which fixes the flaw exploited by the 'MSBlast' (or LoveSan) worm.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8460
BID	8458
CVE	CVE-2003-0605
CVE	CVE-2003-0528
CVE	CVE-2003-0715
XREF	MSFT:MS03-039

XREF	IAVA:2003-A-0012
XREF	OSVDB:2535
XREF	OSVDB:11797
XREF	OSVDB:11460

Ports

tcp/445

22194 - MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)

Description

The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.7 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	19409
CVE	CVE-2006-3439
XREF	MSFT:MS06-040
XREF	IAVA:2006-A-0036
XREF	OSVDB:27845

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

19408 - MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check)

Description

The remote version of Windows contains a flaw in the function 'PNP_QueryResConfList()' in the Plug and Play service that may allow an attacker to execute arbitrary code on the remote host with SYSTEM privileges.
A series of worms (Zotob) are known to exploit this vulnerability in the wild.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	14513
CVE	CVE-2005-1983
XREF	MSFT:MS05-039

XREF	IAVA:2005-A-0025
XREF	OSVDB:18605

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

21193 - MS05-047: Plug and Play Remote Code Execution and Local Privilege Elevation (905749) (uncredentialed check)

Description

The remote host contain a version of the Plug and Play service that contains a vulnerability in the way it handles user-supplied data.
An authenticated attacker may exploit this flaw by sending a malformed RPC request to the remote service and execute code with SYSTEM privileges.
Note that authentication is not required against Windows 2000 if the MS05-039 patch is missing.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	15065
CVE	CVE-2005-2120
XREF	MSFT:MS05-047
XREF	OSVDB:18830

Exploitable with

Core Impact (true)

Ports

tcp/445

18490 - MS05-025: Cumulative Security Update for Internet Explorer (883939)

Description

The remote host is missing IE Cumulative Security Update 883939.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	13941
BID	13943
BID	13946
BID	13947
BID	5560

CVE	CVE-2002-0648
CVE	CVE-2005-1211
XREF	MSFT:MS05-025
XREF	IAVA:2005-A-0016
XREF	IAVA:2001-A-0015
XREF	OSVDB:5162
XREF	OSVDB:17314
XREF	OSVDB:17313

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3828.2700
```

20299 - MS05-054: Cumulative Security Update for Internet Explorer (905915)

Description

The remote host is missing IE Cumulative Security Update 905915.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	16409
BID	15827
BID	15825
BID	15823
BID	13799
CVE	CVE-2006-0057
CVE	CVE-2005-2831
CVE	CVE-2005-2830
CVE	CVE-2005-2829
CVE	CVE-2005-1790
XREF	MSFT:MS05-054
XREF	IAVA:2005-A-0042

XREF	OSVDB:23657
XREF	OSVDB:21763
XREF	OSVDB:21762
XREF	OSVDB:21761
XREF	OSVDB:21760
XREF	OSVDB:17094

Exploitable with

Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3835.2200
```

24333 - MS07-009: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (927779)

Description

The remote host contains a version of the ADODB.Connection ActiveX control that is vulnerable to a security flaw that could allow an attacker to execute arbitrary code on the remote host by constructing a malicious web page and entice a victim to visit this web page.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	20704
CVE	CVE-2006-5559
XREF	MSFT:MS07-009
XREF	IAVA:2007-A-0015
XREF	OSVDB:31882

Ports

tcp/445

```
- C:\Program Files\Common Files\system\ado\\msado15.dll has not been patched
    Remote version : 2.53.6200.0
    Should be : 2.53.6307.0
```

19401 - MS05-038: Cumulative Security Update for Internet Explorer (896727)

Description

The remote host contains a version of the Internet Explorer that is vulnerable to multiple security flaws (JPEG Rendering, Web Folder, COM Object) that could allow an attacker to execute arbitrary code on the remote host by constructing a malicious web page and entice a victim to visit this web page.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	14515
BID	14512
BID	14511
CVE	CVE-2005-1990
CVE	CVE-2005-1989
CVE	CVE-2005-1988
XREF	MSFT:MS05-038
XREF	IAVA:2005-A-0024
XREF	OSVDB:18612
XREF	OSVDB:18611
XREF	OSVDB:18610

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3831.1800
```

36153 - MS09-015: Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426)

Description

A vulnerability in the way the Windows SearchPath function locates and opens files on the remote host could allow an attacker to execute arbitrary remote code if he can trick a user into downloading a specially crafted file into a specific location, such as the Windows Desktop.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	29445
CVE	CVE-2008-2540
XREF	CWE:264

XREF	MSFT:MS09-015
XREF	IAVA:2009-A-0035
XREF	OSVDB:53623

Ports
tcp/445

```
- C:\WINNT\System32\Secur32.dll has not been patched
    Remote version : 5.0.2195.6695
    Should be : 5.0.2195.7244
```

42109 - MS09-053: Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution (975254)

Description

The remote host has a version of IIS whose FTP service is affected by one or both of the following vulnerabilities :
- By sending specially crafted list commands to the remote Microsoft FTP service, an attacker is able to cause the service to become unresponsive. (CVE-2009-2521)
- A flaw in the way the installed Microsoft FTP service in IIS handles list commands can be exploited to execute remote commands in the context of the LocalSystem account with IIS 5.0 under Windows 2000 or to cause the FTP server to stop and become unresponsive with IIS 5.1 under Windows XP or IIS 6.0 under Windows 2003. (CVE-2009-3023)

Risk Factor

High

CVSS Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

References

BID	36189
BID	36273
CVE	CVE-2009-3023
CVE	CVE-2009-2521
XREF	MSFT:MS09-053
XREF	OSVDB:57753
XREF	OSVDB:57589
XREF	CWE:119
XREF	EDB-ID:17476

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports
tcp/445

```
- C:\WINNT\System32\inetsrv\ftpsvc2.dll has not been patched
    Remote version : 5.0.2195.6628
    Should be : 5.0.2195.7336
```

40556 - MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908)

Description

The remote Windows host contains a version of the Microsoft Active Template Library (ATL), included as part of Visual Studio or Visual C++, that is affected by multiple vulnerabilities :
- A remote code execution issue affects the Microsoft Video ActiveX Control due to the a flaw in the function 'CComVariant::ReadFromStream' used in the ATL header, which fails to properly restrict untrusted data read from a stream. (CVE-2008-0015)
- A remote code execution issue exists in the Microsoft Active Template Library due to an error in the 'Load' method of the 'IPersistStreamInit' interface, which could allow calls to 'memcpy' with untrusted data.
(CVE-2008-0020)
- An issue in the ATL headers could allow an attacker to force VariantClear to be called on a VARIANT that has not been correctly initialized and, by supplying a corrupt stream, to execute arbitrary code.
(CVE-2009-0901)
- Unsafe usage of 'OleLoadFromStream' could allow instantiation of arbitrary objects which can bypass related security policy, such as kill bits within Internet Explorer. (CVE-2009-2493)
- A bug in the ATL header could allow reading a variant from a stream and leaving the variant type read with an invalid variant, which could be leveraged by an attacker to execute arbitrary code remotely.
(CVE-2009-2494)

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	35982
BID	35832
BID	35828
BID	35585
BID	35558
CVE	CVE-2009-2494
CVE	CVE-2009-2493
CVE	CVE-2009-0901
CVE	CVE-2008-0020
CVE	CVE-2008-0015
XREF	CWE:94
XREF	MSFT:MS09-037
XREF	IAVA:2009-A-0127
XREF	IAVA:2009-A-0097
XREF	IAVA:2009-A-0094
XREF	IAVA:2009-A-0067
XREF	IAVA:2009-A-0063
XREF	IAVA:2009-A-0061

XREF	IAVA:2009-A-0051
XREF	OSVDB:56910
XREF	OSVDB:56698
XREF	OSVDB:56696
XREF	OSVDB:56272
XREF	OSVDB:55651

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\System32\Atl.dll has not been patched
    Remote version : 3.0.9435.0
    Should be : 3.0.9793.0
```

31044 - MS08-010: Cumulative Security Update for Internet Explorer (944533)

Description

The remote host is missing the IE cumulative security update 944533.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	27689
BID	27668
BID	27666
BID	25977
BID	25571
CVE	CVE-2008-0078
CVE	CVE-2008-0077
CVE	CVE-2008-0076
CVE	CVE-2007-5322
CVE	CVE-2007-4790
XREF	CWE:119
XREF	MSFT:MS08-010
XREF	IAVA:2008-A-0008

XREF	OSVDB:41468
XREF	OSVDB:41467
XREF	OSVDB:41466
XREF	OSVDB:41465
XREF	OSVDB:38487

Ports
tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3860.1000
```

39342 - MS09-020: Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483)

Description

Due to a flaw in the WebDAV extension for IIS, an anonymous, remote attacker may be able to bypass authentication by sending a specially crafted HTTP request and gain access to a protected location.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	34993
CVE	CVE-2009-1535
CVE	CVE-2009-1122
XREF	CWE:287
XREF	MSFT:MS09-020
XREF	OSVDB:56474
XREF	OSVDB:54555

Ports
tcp/445

```
- C:\WINNT\system32\inetsrv\Httpext.dll has not been patched
    Remote version : 5.0.2195.6692
    Should be : 5.0.2195.7290
```

21694 - MS06-032: Vulnerability in TCP/IP Could Allow Remote Code Execution (917953)

Description

The remote version of Windows contains a version of the TCP/IP protocol that is vulnerable to a buffer overflow attack.
An attacker may exploit these flaws to execute code on the remote host.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	18374
CVE	CVE-2006-2379
XREF	MSFT:MS06-032
XREF	OSVDB:26433

Ports

tcp/445

```
- C:\WINNT\system32\drivers\Tcpip.sys has not been patched
    Remote version : 5.0.2195.6706
    Should be : 5.0.2195.7087
```

22193 - MS06-051: Vulnerability in Windows Kernel Could Result in Remote Code Execution (917422)

Description

The remote host contains a version of the Windows kernel that could allow a local user to elevate his privileges or to crash it (therefore causing a denial of service).

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	19384
BID	19375
CVE	CVE-2006-3648
CVE	CVE-2006-3443
XREF	MSFT:MS06-051
XREF	OSVDB:27847
XREF	OSVDB:27846
XREF	CWE:264

Ports

tcp/445

```
- C:\WINNT\system32\Kernel32.dll has not been patched
    Remote version : 5.0.2195.6688
    Should be : 5.0.2195.7099
```

13637 - MS04-019: Utility Manager Could Allow Code Execution (842526)

Description

The remote host is running a version of the Utility Manager that could allow a local attacker to execute arbitrary code on the host, thus escalating his privileges and obtaining the full control of the remote system.

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

BID	10707
CVE	CVE-2004-0213
XREF	MSFT:MS04-019
XREF	OSVDB:7792

Ports

tcp/445

```
- C:\WINNT\system32\Umandlg.dll has not been patched
    Remote version : 1.0.0.3
    Should be : 1.0.0.5
```

44417 - MS10-007: Vulnerability in Windows Shell Handler Could Allow Remote Code Execution (975713)

Description

The ShellExecute() API function on the remote host fails to properly validate URLs, which could result in arbitrary code execution.
A remote attacker could exploit this by tricking a user into making an application (e.g. web browser) pass specially crafted data to the vulnerable function, resulting in remote code execution.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	37884
CVE	CVE-2010-0027
XREF	CWE:94
XREF	MSFT:MS10-007
XREF	IAVA:2010-A-0029
XREF	IAVA:2010-A-0014
XREF	OSVDB:62245

Ports

tcp/445

```
- C:\WINNT\system32\Shlwapi.dll has not been patched
    Remote version : 5.0.3502.6601
    Should be : 5.0.3900.7349
```

25166 - MS07-027: Cumulative Security Update for Internet Explorer (931768)

Description

The remote host is missing the IE cumulative security update 931768.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	23827
BID	23772
BID	23771
BID	23770
BID	23769
BID	23331
CVE	CVE-2007-2221
CVE	CVE-2007-0947
CVE	CVE-2007-0946
CVE	CVE-2007-0945
CVE	CVE-2007-0944
CVE	CVE-2007-0942
CVE	CVE-2007-0323
XREF	MSFT:MS07-027
XREF	IAVA:2007-A-0032
XREF	OSVDB:35873
XREF	OSVDB:34404
XREF	OSVDB:34403
XREF	OSVDB:34402
XREF	OSVDB:34401
XREF	OSVDB:34400
XREF	OSVDB:34399

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
```

```
Remote version : 5.0.3700.6699
Should be : 5.0.3850.1900
```

16326 - MS05-011: Vulnerability in SMB may allow remote code execution (885250)

Description

The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that could allow an attacker to execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to send malformed responses to the remote SMB client, and would be able to either execute arbitrary code on the remote host or to perform a denial of service.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	12484
CVE	CVE-2005-0045
XREF	MSFT:MS05-011
XREF	OSVDB:13600

Exploitable with

CANVAS (true)

Ports

tcp/445

```
- C:\WINNT\system32\drivers\Mrxsmb.sys has not been patched
    Remote version : 5.0.2195.6713
    Should be : 5.0.2195.7023
```

45513 - MS10-026: Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (977816)

Description

The Microsoft MPEG Layer-3 (MP3) codecs have a buffer overflow vulnerability that is triggered by opening a specially crafted AVI file with an MP3 audio stream.
A remote attacker could exploit this by tricking a user into opening a malicious AVI file, which would lead to arbitrary code execution.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	39303
CVE	CVE-2010-0480
XREF	MSFT:MS10-026
XREF	IAVA:2010-A-0053

XREF	OSVDB:63749

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\L3codecx.ax has not been patched
    Remote version : 1.5.0.50
    Should be : 1.6.0.51
```

40889 - MS09-046: Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (956844)

Description

The remote host is missing Security Update 956844. The DHTML Editing Component ActiveX Control on the remote host has a remote code execution vulnerability. A remote attacker could exploit this by tricking a user into viewing a specially crafted web page, resulting in the execution of arbitrary code.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	36280
CVE	CVE-2009-2519
XREF	CWE:94
XREF	MSFT:MS09-046
XREF	IAVA:2009-A-0075
XREF	OSVDB:57798

Ports

tcp/445

```
- C:\Program Files\Common Files\Microsoft Shared\Triedit\Triedit.dll has not been patched
    Remote version : 6.1.0.8594
    Should be : 6.1.0.9235
```

22536 - MS06-063: Vulnerability in Server Service Could Allow Denial of Service (923414)

Description

The remote host has a memory corruption vulnerability in the 'Server' service that could allow an attacker to perform a denial of service against the remote host.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	20373
BID	19215
CVE	CVE-2006-4696
CVE	CVE-2006-3942
CVE	CVE-2006-1315
CVE	CVE-2006-1314
XREF	MSFT:MS06-063
XREF	OSVDB:29439
XREF	OSVDB:27644
XREF	OSVDB:27155
XREF	OSVDB:27154
XREF	CWE:94

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\drivers\Srv.sys has not been patched
    Remote version : 5.0.2195.6699
    Should be : 5.0.2195.7106
```

22188 - MS06-046: Vulnerability in HTML Help Could Allow Remote Code Execution (922616)

Description

The remote host contains a version of the HTML Help ActiveX control that could allow an attacker to execute arbitrary code on the remote host by constructing a malicious web page and entice a victim to visit this web page.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	18769
CVE	CVE-2006-3357
XREF	MSFT:MS06-046
XREF	IAVA:2006-A-0039
XREF	OSVDB:26835

Ports

tcp/445

```
- C:\WINNT\system32\Hhctrl.ocx has not been patched
    Remote version : 5.2.3735.1
```

```
    Should be : 5.2.3790.558
```

22530 - MS06-057: Vulnerability in Windows Explorer Could Allow Remote Execution (923191)

Description

The remote host is running a version of Windows that contains a flaw in the Windows Explorer WebViewFolderIcon ActiveX control (Web View).
An attacker may be able to execute arbitrary code on the remote host by constructing a malicious script and enticing a victim to visit a web site or view a specially crafted email message.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2006-4690
XREF	MSFT:MS06-057

Ports

tcp/445

```
- C:\WINNT\system32\Comctl32.dll has not been patched
    Remote version : 5.81.3502.6601
    Should be : 5.81.3900.7109
```

22029 - MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159)

Description

The remote host is vulnerable to heap overflow in the 'Server' service that could allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.
In addition to this, the remote host is also vulnerable to an information disclosure attack in SMB that could allow an attacker to obtain portions of the memory of the remote host.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	18863
BID	18891
CVE	CVE-2006-1315
CVE	CVE-2006-1314
XREF	MSFT:MS06-035
XREF	OSVDB:27155
XREF	OSVDB:27154

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\drivers\Srv.sys has not been patched
    Remote version : 5.0.2195.6699
    Should be : 5.0.2195.7087
```

23833 - MS06-072: Cumulative Security Update for Internet Explorer (925454)

Description

The remote host is missing the IE cumulative security update 925454.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.
Note that Microsoft has re-released this hotfix as its initial version contained a buffer overflow.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	21494
BID	21546
BID	21507
BID	21552
CVE	CVE-2006-5577
CVE	CVE-2006-5578
CVE	CVE-2006-5581
CVE	CVE-2006-5579
XREF	MSFT:MS06-072
XREF	IAVA:2006-A-0055
XREF	OSVDB:30816
XREF	OSVDB:30815
XREF	OSVDB:30814
XREF	OSVDB:30813

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3846.2300
```

31797 - MS08-024: Cumulative Security Update for Internet Explorer (947864)

Description

The remote host is missing the IE cumulative security update 947864.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	28552
CVE	CVE-2008-1085
XREF	CWE:94
XREF	MSFT:MS08-024
XREF	IAVA:2008-A-0017
XREF	OSVDB:44205

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3862.1500
```

25484 - MS07-031: Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840)

Description

The remote host is running a version of Windows that has a bug in the SSL/TLS server-key exchange handling routine that may allow an attacker to execute arbitrary code on the remote host by luring a user on the remote host into visiting a rogue web site.
On Windows 2000 and 2003 this vulnerability only results in a crash of the web browser.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	24416
CVE	CVE-2007-2218
XREF	MSFT:MS07-031
XREF	IAVA:2007-A-0033
XREF	OSVDB:35347

Ports

tcp/445

```
- C:\WINNT\System32\Schannel.dll has not been patched
    Remote version : 5.1.2195.6705
    Should be : 5.1.2195.7136
```

22449 - MS06-055: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (925486)

Description

The remote host is running a version of Internet Explorer or Outlook Express that is vulnerable to a bug in the Vector Markup Language (VML) handling routine that could allow an attacker execute arbitrary code on the remote host by sending a specially crafted email or by luring a user on the remote host into visiting a rogue web site.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	20096
CVE	CVE-2006-4868
XREF	MSFT:MS06-055
XREF	IAVA:2006-A-0041
XREF	OSVDB:28946

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\Program Files\Common Files\Microsoft Shared\VGX\Vgx.dll has not been patched
    Remote version : 5.0.3014.1003
    Should be : 5.0.3845.1800
```

40557 - MS09-038: Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution (971557)

Description

The remote Windows host is affected by two vulnerabilities involving the way in which AVI headers are processed and AVI data is validated that could be abused to execute arbitrary code remotely.
If an attacker can trick a user on the affected system into opening a specially crafted AVI file, he may be able to leverage these issues to execute arbitrary code subject to the user's privileges.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	35970
BID	35967
CVE	CVE-2009-1546
CVE	CVE-2009-1545
XREF	CWE:189
XREF	MSFT:MS09-038

XREF	IAVA:2009-A-0068
XREF	OSVDB:56909
XREF	OSVDB:56908

Ports
tcp/445

```
- C:\WINNT\System32\Avifil32.dll has not been patched
    Remote version : 5.0.2195.6612
    Should be : 5.0.2195.7316
```

34743 - MS08-068: Vulnerability in SMB Could Allow Remote Code Execution (957097)

Description

The remote version of Windows contains a version of SMB (Server Message Block) protocol that is vulnerable to a credentials reflection attack.
An attacker may exploit this flaw to elevate his privileges and gain control of the remote host.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.3 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	7385
CVE	CVE-2008-4037
XREF	MSFT:MS08-068
XREF	OSVDB:49736
XREF	CWE:287

Exploitable with

Core Impact (true)Metasploit (true)

Ports
tcp/445

```
- C:\WINNT\system32\drivers\Mrxsmb.sys has not been patched
    Remote version : 5.0.2195.6713
    Should be : 5.0.2195.7174
```

20906 - MS06-006: Vulnerability in Windows Media Player Plug-in Could Allow Remote Code Execution (911564)

Description

The remote host is running the Windows Media Player plug-in.
There is a vulnerability in the remote version of this software that could allow an attacker to execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to send a specially crafted media file with a rogue EMBED element and have a user on the affected host open it with the plug-in.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	16644
CVE	CVE-2006-0005
XREF	MSFT:MS06-006
XREF	OSVDB:23132
XREF	CWE:119

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\Program Files\Windows Media Player\Npdsplay.dll has not been patched
    Remote version : 3.0.2.628
    Should be : 3.0.2.629
```

29313 - MS07-069: Cumulative Security Update for Internet Explorer (942615)

Description

The remote host is missing the IE cumulative security update 942615.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	26819
BID	26817
BID	26816
BID	26815
BID	26506
BID	26427
BID	25544
CVE	CVE-2007-6387
CVE	CVE-2007-5347
CVE	CVE-2007-5344
CVE	CVE-2007-4471
CVE	CVE-2007-3903

CVE	CVE-2007-3902
CVE	CVE-2007-0322
XREF	CWE:119
XREF	MSFT:MS07-069
XREF	IAVA:2007-A-0057
XREF	OSVDB:42613
XREF	OSVDB:39121
XREF	OSVDB:39120
XREF	OSVDB:39119
XREF	OSVDB:39118
XREF	OSVDB:37243
XREF	OSVDB:37134

Ports
tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3858.1100
```

33874 - MS08-045: Cumulative Security Update for Internet Explorer (953838)

Description

The remote host is missing the IE cumulative security update 953838.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	30614
BID	30613
BID	30612
BID	30611
BID	30610
BID	28295
CVE	CVE-2008-2259
CVE	CVE-2008-2258

CVE	CVE-2008-2257
CVE	CVE-2008-2256
CVE	CVE-2008-2255
CVE	CVE-2008-2254
XREF	CWE:399
XREF	MSFT:MS08-045
XREF	IAVA:2008-A-0059
XREF	OSVDB:47419
XREF	OSVDB:47418
XREF	OSVDB:47417
XREF	OSVDB:47416
XREF	OSVDB:47415
XREF	OSVDB:47414

Ports
tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3866.2000
```

11928 - MS03-044: Buffer Overrun in Windows Help (825119)

Description
A security vulnerability exists in the Windows Help Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could run code with Local System privileges on this host.

Risk Factor
High

CVSS Base Score
9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score
6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References
BID	8828
CVE	CVE-2003-0711
XREF	MSFT:MS03-044
XREF	OSVDB:11462

Ports
tcp/445

```
- C:\WINNT\system32\itircl.dll has not been patched
    Remote version : 5.2.3644.0
    Should be : 5.2.3790.80
```

16124 - MS05-002: Cursor and Icon Format Handling Code Execution (891711)

Description

The remote host contains a version of the Windows kernel that is affected by a security flaw in the way that cursors and icons are handled. An attacker may be able to execute arbitrary code on the remote host by constructing a malicious web page and entice a victim to visit this web page. An attacker may send a malicious email to the victim to exploit this flaw too.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	12233
BID	12095
CVE	CVE-2005-0416
CVE	CVE-2004-1305
CVE	CVE-2004-1049
XREF	MSFT:MS05-002
XREF	IAVA:2005-A-0001
XREF	OSVDB:16430
XREF	OSVDB:12842
XREF	OSVDB:12624
XREF	OSVDB:12623

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\User32.dll has not been patched
    Remote version : 5.0.2195.6688
    Should be : 5.0.2195.7017
```

21689 - MS06-025: Vulnerability in Routing and Remote Access Could Allow Remote Code Execution (911280)

Description

The remote version of Windows contains a version of RRAS (Routing and Remote Access Service) that has several memory corruption vulnerabilities.
An attacker may exploit these flaws to execute code on the remote service.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	18424
BID	18358
BID	18325
CVE	CVE-2006-2371
CVE	CVE-2006-2370
XREF	MSFT:MS06-025
XREF	OSVDB:26437
XREF	OSVDB:26436

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Rasmans.dll has not been patched
    Remote version : 5.0.2195.6696
    Should be : 5.0.2195.7093
```

23645 - MS06-068: Vulnerability in Microsoft Agent Could Remote Code Execution (920213)

Description

The remote version of Windows contains a flaw in the Microsoft Agent service that could allow an attacker to execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to set up a rogue web site and lure a victim on the remote host into visiting it or have him load a malformed .ACF file.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	21034
CVE	CVE-2006-3445
XREF	MSFT:MS06-068
XREF	OSVDB:30262

Ports

tcp/445

```
- C:\WINNT\msagent\Agentsvr.exe has not been patched
    Remote version : 2.0.0.3422
    Should be : 2.0.0.3424
```

18023 - MS05-019: Vulnerabilities in TCP/IP Could Allow Remote Code Execution (893066)

Description

The remote host runs a version of Windows that has a flaw in its TCP/IP stack.
The flaw could allow an attacker to execute arbitrary code with SYSTEM privileges on the remote host, or to perform a denial of service attack against the remote host.
Proof of concept code is available to perform a Denial of Service against a vulnerable system.

Risk Factor

High

CVSS Base Score

9.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:C)

CVSS Temporal Score

6.7 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:C)

References

BID	13658
BID	13124
BID	13116
CVE	CVE-2005-0688
CVE	CVE-2005-0068
CVE	CVE-2005-0067
CVE	CVE-2005-0066
CVE	CVE-2005-0065
CVE	CVE-2005-0048
CVE	CVE-2004-1060
CVE	CVE-2004-0790
CVE	CVE-2004-0230
XREF	MSFT:MS05-019
XREF	IAVA:2004-A-0007
XREF	OSVDB:4030
XREF	OSVDB:15623
XREF	OSVDB:15622
XREF	OSVDB:15621
XREF	OSVDB:15620
XREF	OSVDB:15619
XREF	OSVDB:15463
XREF	OSVDB:15457
XREF	OSVDB:14578

Ports

tcp/445

```
- C:\WINNT\system32\drivers\Tcpip.sys has not been patched
    Remote version : 5.0.2195.6706
    Should be : 5.0.2195.7049
```

26963 - MS07-057: Cumulative Security Update for Internet Explorer (939653)

Description

The remote host is missing the IE cumulative security update 939653.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	25916
BID	25915
BID	24911
BID	22680
CVE	CVE-2007-3893
CVE	CVE-2007-3892
CVE	CVE-2007-3826
CVE	CVE-2007-1091
XREF	MSFT:MS07-057
XREF	IAVA:2007-A-0046
XREF	OSVDB:38212
XREF	OSVDB:37626
XREF	OSVDB:37625
XREF	OSVDB:32087

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3856.1700
```

22030 - MS06-036: Vulnerability in DHCP Client Service Could Allow Remote Code Execution (914388)

Description

The remote host contains a DHCP client which is vulnerable to a buffer overrun attack when receiving a malformed response to a DHCP request.
An attacker could exploit this flaw to execute arbitrary code on the remote host with 'SYSTEM' privileges.
Typically, the attacker would need to be on the same physical subnet as this victim to exploit this flaw. Also, the victim needs to be configured to use DHCP.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	18923
CVE	CVE-2006-2372
XREF	MSFT:MS06-036
XREF	OSVDB:27151
XREF	CWE:119

Ports

tcp/445

```
- C:\WINNT\system32\Dhcpcsvc.dll has not been patched
    Remote version : 5.0.2195.6685
    Should be : 5.0.2195.7085
```

42439 - MS09-065: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947)

Description

The remote host contains a version of the Windows kernel that is affected by multiple vulnerabilities :
- A NULL pointer dereferencing vulnerability allowing a local user to elevate his privileges (CVE-2009-1127)
- Insufficient validation of certain input passed to GDI from user mode allows a local user to run arbitrary code in kernel mode. (CVE-2009-2513)
- A parsing vulnerability when decoding a specially crafted Embedded OpenType (EOT) font may allow a remote user to execute arbitrary code on the remote host by luring a user of the remote host into viewing a web page containing such a malformed font. (CVE-2009-2514)

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	36941
BID	36939
BID	36029
CVE	CVE-2009-2514
CVE	CVE-2009-2513
CVE	CVE-2009-1127
XREF	CWE:94
XREF	MSFT:MS09-065

XREF	IAVA:2009-A-0117
XREF	OSVDB:59869
XREF	OSVDB:59868
XREF	OSVDB:59867

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\Win32k.sys has not been patched
    Remote version : 5.0.2195.6708
    Should be : 5.0.2195.7322
```

44415 - MS10-005: Vulnerability in Microsoft Paint Could Allow Remote Code Execution (978706)

Description

The remote Windows host is running a version of Microsoft Paint that has an integer overflow vulnerability that can be triggered when decoding JPEG images.
If an attacker can trick a user on the affected host into opening a specially crafted JPEG image file using Microsoft Paint, he may be able to leverage these issues to execute arbitrary code subject to the user's privileges.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.3 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	38042
CVE	CVE-2010-0028
XREF	CWE:189
XREF	MSFT:MS10-005
XREF	OSVDB:62242

Ports

tcp/445

```
- C:\WINNT\system32\Mspaint.exe has not been patched
    Remote version : 5.0.2195.6601
    Should be : 5.0.2195.7368
```

46842 - MS10-035: Cumulative Security Update for Internet Explorer (982381)

Description

The remote host is missing IE Security Update 982381.
The remote version of IE is affected by several vulnerabilities that may allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	40417
BID	40416
BID	40414
BID	40410
BID	38056
BID	38055
CVE	CVE-2010-1262
CVE	CVE-2010-1261
CVE	CVE-2010-1260
CVE	CVE-2010-1259
CVE	CVE-2010-1257
CVE	CVE-2010-0255
XREF	CWE:264
XREF	MSFT:MS10-035
XREF	IAVA:2010-A-0080
XREF	IAVA:2010-A-0079
XREF	OSVDB:65215
XREF	OSVDB:65214
XREF	OSVDB:65213
XREF	OSVDB:65212
XREF	OSVDB:65211
XREF	OSVDB:62156

Exploitable with

CANVAS (true)

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3888.1400
```

20298 - MS05-055: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (908523)

Description

The remote host contains a version of the Windows kernel that may allow a local user to elevate his privileges or to crash it (therefore causing a denial of service).

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

BID	15826
CVE	CVE-2005-2827
XREF	MSFT:MS05-055
XREF	OSVDB:18823

Ports

tcp/445

```
- C:\WINNT\system32\Ntoskrnl.exe has not been patched
    Remote version : 5.0.2195.6717
    Should be : 5.0.2195.7071
```

36150 - MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)

Description

The version of Windows running on the remote host is affected by potentially four vulnerabilities involving its MSDTC transaction facility and/or Windows Service Isolation that may allow a local user to escalate his privileges and take complete control of the affected system.

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

BID	34444
BID	34443
BID	34442
BID	28833
CVE	CVE-2009-0080
CVE	CVE-2009-0079
CVE	CVE-2009-0078
CVE	CVE-2008-1436
XREF	MSFT:MS09-012
XREF	OSVDB:53668
XREF	OSVDB:53667
XREF	OSVDB:53666
XREF	OSVDB:44580

XREF	CWE:264

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\System32\Msdtcprx.dll has not been patched
    Remote version : 2000.2.3504.0
    Should be : 2000.2.3549.0
```

33875 - MS08-046: Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution (952954)

Description

The remote host contains a version of the Color Management Module that is vulnerable to a security flaw which could allow an attacker to execute arbitrary code on the remote host by crafting a malformed image file and entice a victim to open it.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	30594
CVE	CVE-2008-2245
XREF	CWE:119
XREF	MSFT:MS08-046
XREF	IAVA:2008-A-0060
XREF	OSVDB:47395

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\Mscms.dll has not been patched
    Remote version : 5.0.2180.1
    Should be : 5.0.2195.7162
```

36151 - MS09-013: Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)

Description

The version of Windows HTTP Services installed on the remote host is affected by several vulnerabilities :
- An integer underflow triggered by a specially crafted response from a malicious web server (for example, during device discovery of UPnP devices on a network) may allow for arbitrary code execution. (CVE-2009-0086)
- Incomplete validation of the distinguished name in a digital certificate may, in combination with other attacks, allow an attacker to successfully spoof the digital certificate of a third-party web site. (CVE-2009-0089)
- A flaw in the way that Windows HTTP Services handles NTLM credentials may allow an attacker to reflect back a user's credentials and thereby gain access as that user. (CVE-2009-0550)

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	34439
BID	34437
BID	34435
CVE	CVE-2009-0550
CVE	CVE-2009-0089
CVE	CVE-2009-0086
XREF	CWE:20
XREF	MSFT:MS09-013
XREF	IAVA:2009-A-0035
XREF	IAVA:2009-A-0034
XREF	OSVDB:53621
XREF	OSVDB:53620
XREF	OSVDB:53619

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\System32\Winhttp.dll has not been patched
    Remote version : 5.1.2600.1188
    Should be : 5.1.2600.3490
```

39791 - MS09-028: Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution (971633)

Description

The DirectShow component included with the version of Microsoft DirectX installed on the remote host is affected by multiple vulnerabilities that may allow execution of arbitrary code when processing a specially crafted QuickTime media file.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	35616

BID	35600
BID	35139
CVE	CVE-2009-1539
CVE	CVE-2009-1538
CVE	CVE-2009-1537
XREF	CWE:94
XREF	MSFT:MS09-028
XREF	IAVA:2009-A-0050
XREF	OSVDB:55845
XREF	OSVDB:55844
XREF	OSVDB:54797

Exploitable with

CANVAS (true)Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\System32\Quartz.dll has not been patched
    Remote version : 6.1.9.728
    Should be : 6.1.9.736
```

25886 - MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)

Description

The remote host is running a version of Internet Explorer or Outlook Express with a bug in the Vector Markup Language (VML) handling routine that may allow an attacker execute arbitrary code on the remote host by sending a specially crafted email or by luring a user on the remote host into visiting a rogue web site.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	25310
CVE	CVE-2007-1749
XREF	MSFT:MS07-050
XREF	IAVA:2007-A-0045
XREF	OSVDB:36390

Ports

tcp/445

```
- C:\Program Files\Common Files\Microsoft Shared\VGX\Vgx.dll has not been patched
    Remote version : 5.0.3014.1003
```

```
Should be : 5.0.3854.2500
```

24911 - MS07-017: Vulnerabilities in GDI Could Allow Remote Code Execution (925902)

Description

The remote host is running a version of Windows with a bug in the Animated Cursor (ANI) handling routine that could allow an attacker to execute arbitrary code on the remote host by sending a specially crafted email or by luring a user on the remote host into visiting a rogue web site.
Additionally, the system is vulnerable to :
- Local Privilege Elevation (GDI, EMF, Font Rasterizer)
- Denial of Service (WMF)

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	23278
BID	23277
BID	23276
BID	23275
BID	23273
BID	23194
CVE	CVE-2007-1765
CVE	CVE-2007-1215
CVE	CVE-2007-1213
CVE	CVE-2007-1212
CVE	CVE-2007-1211
CVE	CVE-2007-0038
CVE	CVE-2006-5758
CVE	CVE-2006-5586
XREF	MSFT:MS07-017
XREF	IAVA:2007-A-0020
XREF	OSVDB:34099
XREF	OSVDB:34098
XREF	OSVDB:34097
XREF	OSVDB:34096
XREF	OSVDB:34095
XREF	OSVDB:33629
XREF	OSVDB:30214

Exploitable with

Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\System32\User32.dll has not been patched
    Remote version : 5.0.2195.6688
    Should be : 5.0.2195.7133
```

23838 - MS06-078: Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689/925398)

Description

The remote host is running Windows Media Player/Series.
There is a vulnerability in the remote version of this software which may allow an attacker to execute arbitrary code on the remote host.
To exploit this flaw, one attacker would need to set up a rogue ASF/ASX file and send it to a victim on the remote host.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	21505
BID	21247
CVE	CVE-2006-6134
CVE	CVE-2006-4702
XREF	MSFT:MS06-078
XREF	IAVA:2006-A-0056
XREF	OSVDB:30819
XREF	OSVDB:30818

Ports

tcp/445

```
- C:\WINNT\system32\Dxmasf.dll has not been patched
    Remote version : 6.4.9.1125
    Should be : 6.4.9.1133
```

35822 - MS09-006: Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)

Description

The remote host contains a version of the Windows kernel that is affected by vulnerabilities :
- A remote code execution vulnerability exists due to improper validation of input passed from user mode through the kernel component of GDI. Successful exploitation requires that a user on the affected host view a specially crafted EMF or WMF image file, perhaps by being tricked into visiting a malicious web site, and could lead to a complete system compromise.
(CVE-2009-0081)
- A local privilege escalation vulnerability exists due to the way the kernel validates handles. (CVE-2009-0082)
- A local privilege escalation vulnerability exists due to improper handling of a specially crafted invalid pointer.
(CVE-2009-0083)

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	34027
BID	34025
BID	34012
CVE	CVE-2009-0083
CVE	CVE-2009-0082
CVE	CVE-2009-0081
XREF	CWE:20
XREF	MSFT:MS09-006
XREF	IAVA:2009-A-0020
XREF	OSVDB:52524
XREF	OSVDB:52523
XREF	OSVDB:52522

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\Win32k.sys has not been patched
    Remote version : 5.0.2195.6708
    Should be : 5.0.2195.7251
```

40407 - MS09-034: Cumulative Security Update for Internet Explorer (972260)

Description

The remote host is missing IE Security Update 972260.
The remote version of IE is affected by several vulnerabilities that may allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	35831
BID	35827

BID	35826
CVE	CVE-2009-1919
CVE	CVE-2009-1918
CVE	CVE-2009-1917
XREF	CWE:94
XREF	MSFT:MS09-034
XREF	IAVA:2009-A-0059
XREF	OSVDB:56695
XREF	OSVDB:56694
XREF	OSVDB:56693

Ports
tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3879.2200
```

20005 - MS05-052: Cumulative Security Update for Internet Explorer (896688)

Description

The remote host contains a version of the Internet Explorer that is vulnerable to a security flaw (COM Object Instantiation Memory Corruption Vulnerability) that could allow an attacker to execute arbitrary code on the remote host by constructing a malicious web page and entice a victim to visit this web page.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	15061
BID	14594
CVE	CVE-2005-2127
XREF	MSFT:MS05-052
XREF	IAVA:2005-A-0028
XREF	OSVDB:2692
XREF	OSVDB:19093

Ports
tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3833.200
```

31794 - MS08-021: Vulnerabilities in GDI Could Allow Remote Code Execution (948590)

Description

The remote host contains a version of Microsoft Windows that is missing a critical security update that fixes several vulnerabilities in the Graphic Rendering Engine, and in the way Windows handles Metafiles.
An attacker may exploit these flaws to execute arbitrary code on the remote host. To exploit this flaw, an attacker would need to send a specially crafted image to a user on the remote host, or lure him into visiting a rogue website containing such a file.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	28571
BID	28570
CVE	CVE-2008-1087
CVE	CVE-2008-1083
XREF	CWE:119
XREF	MSFT:MS08-021
XREF	IAVA:2008-A-0018
XREF	OSVDB:44215
XREF	OSVDB:44214
XREF	OSVDB:44213

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\gdi32.dll has not been patched
    Remote version : 5.0.2195.6660
    Should be : 5.0.2195.7153
```

25883 - MS07-045: Cumulative Security Update for Internet Explorer (937143)

Description

The remote host is missing IE Cumulative Security Update 937143.
The remote version of IE is potentially vulnerable to several flaws that may allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	25312
BID	25311
BID	25295
BID	25289
BID	25288
CVE	CVE-2007-3041
CVE	CVE-2007-2929
CVE	CVE-2007-2928
CVE	CVE-2007-2240
CVE	CVE-2007-2216
CVE	CVE-2007-0943
CVE	CVE-2007-0319
XREF	MSFT:MS07-045
XREF	IAVA:2007-A-0044
XREF	OSVDB:39555
XREF	OSVDB:39554
XREF	OSVDB:39553
XREF	OSVDB:37710
XREF	OSVDB:36397
XREF	OSVDB:36396
XREF	OSVDB:36395

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3854.1200
```

25023 - MS07-020: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168)

Description

The remote version of Windows contains a flaw in the Microsoft Agent service that could allow an attacker to execute code on the remote host.
To exploit this flaw, an attacker would need to set up a rogue web site and lure a victim on the remote host into visiting it.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	23337
CVE	CVE-2007-1205
XREF	MSFT:MS07-020
XREF	IAVA:2007-A-0021
XREF	OSVDB:34009

Ports

tcp/445

```
- C:\WINNT\msagent\Agentdpv.dll has not been patched
    Remote version : 2.0.0.3422
    Should be : 2.0.0.3425
```

18489 - MS05-030: Vulnerability in Outlook Express Could Allow Remote Code Execution (897715)

Description

The remote host is running a version of Microsoft Outlook Express that could allow an attacker to execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to lure a user to connect to a rogue NNTP (news) server sending malformed replies to several queries.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.3 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	13951
CVE	CVE-2005-1213
XREF	MSFT:MS05-030
XREF	OSVDB:17306

Exploitable with

Core Impact (true)Metasploit (true)

Ports

tcp/445

```
Path : C:\Program Files\Outlook Express\msoe.dll
Version : 5.50.4927.1200
Should be : 5.50.4952.2800
```

15964 - MS04-043: Vulnerabilities in HyperTerminal (873339)

Description

The remote host contains a version of the HyperTerminal software that could allow an attacker to execute arbitrary code on the remote host by tricking a victim into using Hyperterminal to log into a rogue host.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	11916
CVE	CVE-2004-0568
XREF	MSFT:MS04-043
XREF	OSVDB:12374

Ports

tcp/445

```
- C:\WINNT\system32\Hypertrm.dll has not been patched
    Remote version : 5.0.2195.6684
    Should be : 5.0.2195.7000
```

45506 - MS10-019: Vulnerabilities in Windows Could Allow Remote Code Execution (981210)

Description

The version of Windows running on the remote host has vulnerabilities in the Windows Authenticode Signature mechanism. Modifying an existing signed executable or cabinet file can result in arbitrary code execution.
A remote attacker could exploit this by tricking a user into executing or opening a maliciously crafted file, resulting in arbitrary code execution.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	39332
BID	39328
CVE	CVE-2010-0487
CVE	CVE-2010-0486
XREF	MSFT:MS10-019
XREF	IAVA:2010-A-0057
XREF	OSVDB:63746
XREF	OSVDB:63745

Ports

tcp/445

```
- C:\WINNT\system32\Wintrust.dll has not been patched
    Remote version : 5.131.2195.6624
    Should be : 5.131.2195.7375
```

22191 - MS06-049: Vulnerability in Windows Kernel Could Result in Elevation of Privilege (920958)

Description

The remote host contains a version of the Windows kernel that could allow a local user to elevate his privileges or to crash it (therefore causing a denial of service).

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	19388
CVE	CVE-2006-3444
XREF	MSFT:MS06-049
XREF	OSVDB:27848

Ports

tcp/445

```
- C:\WINNT\system32\Ntkrnlpa.exe has not been patched
    Remote version : 5.0.2195.6717
    Should be : 5.0.2195.7111
```

23644 - MS06-067: Cumulative Security Update for Internet Explorer (922760)

Description

The remote host is missing the IE cumulative security update 922760.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.
Note that Microsoft has re-released this hotfix as its initial version contained a buffer overflow.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.3 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	21020
CVE	CVE-2006-4687
CVE	CVE-2006-4777
CVE	CVE-2006-4446
XREF	MSFT:MS06-067
XREF	IAVA:2006-A-0053
XREF	OSVDB:31323
XREF	OSVDB:28842
XREF	OSVDB:28841

Exploitable with

Metasploit (true)

Ports
tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3842.3000
```

29894 - MS08-002: Vulnerability in LSASS Could Allow Local Elevation of Privilege (943485)

Description

The remote host is running version of Windows and LSASS that could allow a local user to gain elevated privileged. An attacker who has the ability to execute arbitrary commands on the remote host may exploit this flaw to gain SYSTEM privileges.

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.3 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

BID	27099
CVE	CVE-2007-5352
XREF	MSFT:MS08-002
XREF	OSVDB:40071
XREF	CWE:264

Ports
tcp/445

```
- C:\WINNT\system32\Lsasrv.dll has not been patched
    Remote version : 5.0.2195.6695
    Should be : 5.0.2195.7147
```

22184 - MS06-042: Cumulative Security Update for Internet Explorer (918899)

Description

The remote host is missing IE Cumulative Security Update 918899.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.
Note that Microsoft has re-released this hotfix since the initial version contained a buffer overflow.

See Also

http://support.microsoft.com/kb/923762/

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	19987

BID	19400
BID	19340
BID	19339
BID	19316
BID	19312
BID	19228
BID	18682
BID	18277
BID	11826
CVE	CVE-2006-7066
CVE	CVE-2006-3873
CVE	CVE-2006-3640
CVE	CVE-2006-3639
CVE	CVE-2006-3638
CVE	CVE-2006-3637
CVE	CVE-2006-3451
CVE	CVE-2006-3450
CVE	CVE-2006-3280
CVE	CVE-2004-1166
XREF	CWE:94
XREF	MSFT:MS06-042
XREF	IAVA:2006-A-0037
XREF	OSVDB:30834
XREF	OSVDB:27855
XREF	OSVDB:27854
XREF	OSVDB:27853
XREF	OSVDB:27852
XREF	OSVDB:27851
XREF	OSVDB:27850
XREF	OSVDB:27533
XREF	OSVDB:26956

XREF	OSVDB:12299

Ports
tcp/445

```
- C:\WINNT\system32\Urlmon.dll has not been patched
    Remote version : 5.0.3700.6705
    Should be : 5.0.3844.3000
```

13641 - MS04-023: Vulnerability in HTML Help Could Allow Code Execution (840315)

Description

The remote host is subject to two vulnerabilities in the HTML Help and showHelp modules that could allow an attacker to execute arbitrary code on the remote host.
To exploit these flaws, an attacker would need to set up a rogue website containing a malicious showHelp URL, and would need to lure a user on the remote host to visit it. Once the user visits the web site, a buffer overflow would allow the attacker to execute arbitrary commands with the privileges of the victim user.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.3 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	9320
BID	10705
CVE	CVE-2003-1041
CVE	CVE-2004-0201
XREF	MSFT:MS04-023
XREF	IAVA:2004-A-0012
XREF	OSVDB:7912
XREF	OSVDB:7804
XREF	OSVDB:7803

Ports
tcp/445

```
- C:\WINNT\system32\Itss.dll has not been patched
    Remote version : 5.2.3644.0
    Should be : 5.2.3790.185
```

13642 - MS04-024: Buffer overrun in Windows Shell (839645)

Description

The remote host is running a version of Windows that has a flaw in its shell. An attacker could persuade a user on the remote host to execute a rogue program by using a CLSID instead of a file type, thus fooling the user into thinking that he will not execute an application but simply open a document.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	9510
CVE	CVE-2004-0420
XREF	MSFT:MS04-024
XREF	OSVDB:7802

Ports

tcp/445

```
- C:\WINNT\system32\Shell32.dll has not been patched
    Remote version : 5.0.3700.6705
    Should be : 5.0.3900.6922
```

24332 - MS07-008: Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843)

Description

The remote host contains a version of the HTML Help ActiveX control that is vulnerable to a security flaw that could allow an attacker to execute arbitrary code on the remote host by constructing a malicious web page and entice a victim to visit this web page.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	22478
CVE	CVE-2007-0214
XREF	MSFT:MS07-008
XREF	IAVA:2007-A-0014
XREF	OSVDB:31884

Ports

tcp/445

```
- C:\WINNT\system32\Hhctrl.ocx has not been patched
    Remote version : 5.2.3735.1
    Should be : 5.2.3790.620
```

44423 - MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935)

Description

The version of Microsoft DirectShow installed on the remote host is affected by a heap buffer overflow that can be triggered when parsing AVI media files.
If an attacker can trick a user on the affected host into opening a specially crafted AVI file, he may be able to leverage this issue to execute arbitrary code subject to the user's privileges.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	38112
CVE	CVE-2010-0250
XREF	CWE:119
XREF	MSFT:MS10-013
XREF	IAVA:2010-A-0025
XREF	OSVDB:62257

Ports

tcp/445

```
- C:\WINNT\System32\Avifil32.dll has not been patched
    Remote version : 5.0.2195.6612
    Should be : 5.0.2195.7359
```

23643 - MS06-066: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (923980)

Description

The remote host contains a version of the Client Service for NetWare that is vulnerable to a buffer overflow. An attacker may exploit this to cause a denial of service by sending a malformed IPX packet to the remote host, or to execute arbitrary code by exploiting a flaw in the NetWare client.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	21023
BID	20984
CVE	CVE-2006-4689
CVE	CVE-2006-4688
XREF	MSFT:MS06-066
XREF	OSVDB:30261
XREF	OSVDB:30260

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\drivers\nwrdr.sys has not been patched
    Remote version : 5.0.2195.6667
    Should be : 5.0.2195.7110
```

43065 - MS09-073: Vulnerability in WordPad and Office Text Converters Could Allow Remote Code Execution (975539)

Description

The remote host contains a vulnerable version of Microsoft WordPad, Office, or Office Converter Pack. Opening a specially crafted Word 97 file can result in the execution of arbitrary code. A remote attacker could exploit this by tricking a user into opening a malicious Word file.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	37216
CVE	CVE-2009-2506
XREF	CWE:94
XREF	MSFT:MS09-073
XREF	IAVA:2009-A-0128
XREF	OSVDB:60834

Ports

tcp/445

```
- C:\Program Files\Common Files\Microsoft Shared\TextConv\Mswrd632.wpc has not been patched
    Remote version : 1999.8.7.0
    Should be : 2009.10.31.10
```

35070 - MS08-071: Vulnerabilities in GDI+ Could Allow Remote Code Execution (956802)

Description

The remote host is running a version of Windows that is affected by multiple buffer oveflow vulnerabilities when viewing WMF files, that could allow an attacker to execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to send a malformed WMF file to a user on the remote host and wait for him to open it using an affected Microsoft application.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	32637
BID	32634
CVE	CVE-2008-3465
CVE	CVE-2008-2249
XREF	CWE:119

XREF	MSFT:MS08-071
XREF	IAVA:2008-A-0086
XREF	OSVDB:50562
XREF	OSVDB:50561

Ports
tcp/445

```
- C:\WINNT\system32\Gdi32.dll has not been patched
    Remote version : 5.0.2195.6660
    Should be : 5.0.2195.7205
```

31798 - MS08-025: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693)

Description
The remote host contains a version of the Windows kernel that is vulnerable to a security flaw that could allow a local user to elevate his privileges or to crash it (therefore causing a denial of service).

Risk Factor
High

CVSS Base Score
7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score
6.0 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

BID	28554
CVE	CVE-2008-1084
XREF	MSFT:MS08-025
XREF	OSVDB:44206
XREF	CWE:94

Exploitable with
CANVAS (true)Core Impact (true)

Ports
tcp/445

```
- C:\WINNT\system32\Win32k.sys has not been patched
    Remote version : 5.0.2195.6708
    Should be : 5.0.2195.7154
```

24000 - MS07-004: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (929969)

Description
The remote host is running a version of Internet Explorer or Outlook Express that is vulnerable to a bug in the Vector Markup Language (VML) handling routine that could allow an attacker execute arbitrary code on the remote host by sending a specially crafted email or by luring a user on the remote host into visiting a rogue web site.

Risk Factor
High

CVSS Base Score
9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	21930
CVE	CVE-2007-0024
XREF	MSFT:MS07-004
XREF	IAVA:2007-A-0005
XREF	OSVDB:31250

Exploitable with

CANVAS (true)

Ports

tcp/445

```
- C:\Program Files\Common Files\Microsoft Shared\VGX\Vgx.dll has not been patched
    Remote version : 5.0.3014.1003
    Should be : 5.0.3848.1800
```

43064 - MS09-072: Cumulative Security Update for Internet Explorer (976325)

Description

The remote host is missing IE Security Update 976325.
The remote version of IE is affected by several vulnerabilities that may allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	37213
BID	37212
BID	37188
BID	37085
BID	35828
CVE	CVE-2009-3674
CVE	CVE-2009-3673
CVE	CVE-2009-3672
CVE	CVE-2009-3671
CVE	CVE-2009-2493
XREF	CWE:399
XREF	MSFT:MS09-072
XREF	IAVA:2009-A-0127
XREF	IAVA:2009-A-0097

XREF	IAVA:2009-A-0094
XREF	IAVA:2009-A-0067
XREF	IAVA:2009-A-0063
XREF	IAVA:2009-A-0061
XREF	OSVDB:60839
XREF	OSVDB:60838
XREF	OSVDB:60837
XREF	OSVDB:60490
XREF	OSVDB:56698

Exploitable with

Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3882.2700
```

25486 - MS07-033: Cumulative Security Update for Internet Explorer (933566)

Description

The remote host is missing IE Cumulative Security Update 933566.
The remote version of IE is affected by several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	24429
BID	24426
BID	24423
BID	24418
BID	24372
BID	22966
CVE	CVE-2007-2222
CVE	CVE-2007-1751
CVE	CVE-2007-3027
CVE	CVE-2007-1750

CVE	CVE-2007-1499
CVE	CVE-2007-0218
XREF	CWE:94
XREF	MSFT:MS07-033
XREF	IAVA:2007-A-0034
XREF	OSVDB:35353
XREF	OSVDB:35352
XREF	OSVDB:35351
XREF	OSVDB:35350
XREF	OSVDB:35349
XREF	OSVDB:35348
XREF	OSVDB:34077

Ports
tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3853.3000
```

24337 - MS07-013: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution (918118)

Description

The remote host contains a version of Microsoft Windows and/or Microsoft Office that has a vulnerability in the RichEdit component that could be abused by an attacker to execute arbitrary code on the remote host.
To exploit this vulnerability, an attacker would need to spend a specially crafted RTF file to a user on the remote host and lure him into opening it.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	21876
CVE	CVE-2006-1311
XREF	MSFT:MS07-013
XREF	OSVDB:31886

Ports
tcp/445

```
- C:\WINNT\system32\Riched20.dll has not been patched
    Remote version : 5.30.23.1215
    Should be : 5.30.23.1227
```

10861 - MS02-005: MSIE 5.01 5.5 6.0 Cumulative Patch (890923)

Description

The Cumulative Patch for IE is not applied on the remote host.
Impact of vulnerability: Run code of attacker's choice.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.4 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	3699
CVE	CVE-2002-0057
XREF	MSFT:MS05-020
XREF	MSFT:MS02-005
XREF	OSVDB:3032

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3826.2400
```

26964 - MS07-058: Vulnerability in RPC Could Allow Denial of Service (933729)

Description

The remote version of Windows contains a version of the RPC library protocol that is vulnerable to a denial of service attack in the NTLM authentication field.
An attacker may exploit this flaw to crash the remote RPC server (and the remote system).

Risk Factor

High

CVSS Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

5.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

References

BID	25974
CVE	CVE-2007-2228
XREF	MSFT:MS07-058
XREF	OSVDB:37629
XREF	OSVDB:37628

Ports

tcp/445

```
- C:\WINNT\system32\Rpcrt4.dll has not been patched
    Remote version : 5.0.2195.6701
    Should be : 5.0.2195.7090
```

11886 - MS03-041: Vulnerability in Authenticode Verification Could Allow Remote Code Execution (823182)

Description

The remote host contains a version of the Authenticode Verification module that could allow an attacker to execute arbitrary code on the remote host by constructing a malicious web page and entice a victim to visit this web page.
An attacker may also be able to exploit the vulnerability by sending a malicious HTML email.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	8830
CVE	CVE-2003-0660
XREF	MSFT:MS03-041
XREF	OSVDB:11463

Ports

tcp/445

```
- C:\WINNT\system32\Cryptui.dll has not been patched
    Remote version : 5.131.2195.6628
    Should be : 5.131.2195.6758
```

26961 - MS07-055: Vulnerability in Kodak Image Viewer Could Allow Remote Code Execution (923810)

Description

The remote host is running a version of the Kodak Image Viewer that may allow arbitrary code to be run.
An attacker may use this to execute arbitrary code on this host.
To succeed, the attacker would have to send a rogue file to a user of the remote computer and have it open it with this application.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	25909
CVE	CVE-2007-2217
XREF	MSFT:MS07-055
XREF	OSVDB:37627
XREF	CWE:94

Exploitable with

CANVAS (true)Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\tifflt.dll has not been patched
    Remote version : 5.0.2920.0
    Should be : 5.0.3900.7134
```

29308 - MS07-064: Vulnerabilities in DirectX Could Allow Remote Code Execution (941568)

Description

The remote host contains a version of DirectX that is vulnerable to a remote code execution attack.
To exploit this flaw, an attacker would need to send a malformed AVI, WMV or SAMI file to a user on the remote host and have him open it.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	26804
CVE	CVE-2007-3895
CVE	CVE-2007-3901
XREF	CWE:119
XREF	MSFT:MS07-064
XREF	IAVA:2007-A-0055
XREF	OSVDB:39127
XREF	OSVDB:39126

Exploitable with

Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\quartz.dll has not been patched
    Remote version : 6.1.9.728
    Should be : 6.1.9.733
```

16125 - MS05-003: Indexing Service Code Execution (871250)

Description

The remote host contains a version of the Indexing Service that may allow an attacker to execute arbitrary code on the remote host by constructing a malicious query.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	12228
CVE	CVE-2004-0897

XREF	MSFT:MS05-003
XREF	OSVDB:12832

Ports
tcp/445

```
- C:\WINNT\system32\Ciodm.dll has not been patched
    Remote version : 5.0.2134.1
    Should be : 5.0.2195.6981
```

42114 - MS09-058: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (971486)

Description

The remote Windows host is running a version of the Windows kernel that is affected by multiple vulnerabilities :
- An elevation of privilege vulnerability exists in the Windows kernel due to the incorrect truncation of a 64- bit value to a 32-bit value. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs, view / change / delete data, or create new accounts with full user rights. (CVE-2009-2515)
- An elevation of privilege vulnerability exists in the Windows kernel due to the incorrect truncation of a 64- bit value to a 32-bit value. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs, view / change / delete data, or create new accounts with full user rights. (CVE-2009-2516)
- A denial of service vulnerability exists in the Windows kernel because of the way the kernel handles certain exceptions. An attacker could exploit the vulnerability by running a specially crafted application causing the system to restart. (CVE-2009-2517)

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	36625
BID	36624
BID	36623
CVE	CVE-2009-2517
CVE	CVE-2009-2516
CVE	CVE-2009-2515
XREF	CWE:264
XREF	MSFT:MS09-058
XREF	IAVA:2009-A-0096
XREF	OSVDB:58861
XREF	OSVDB:58860
XREF	OSVDB:58859

Exploitable with

Core Impact (true)

Ports
tcp/445

```
- C:\WINNT\system32\ntoskrnl.exe has not been patched
    Remote version : 5.0.2195.6717
    Should be : 5.0.2195.7319
```

25488 - MS07-035: Vulnerability in Win 32 API Could Allow Remote Code Execution (935839)

Description

The remote host contains a version of the Win32 API that is vulnerable to a security flaw that could allow a local user to elevate his privileges, and might allow a remote attacker to execute arbitrary code on the host.
To exploit the flaw, an attacker would need to find a way to misuse the Win32 API. One way of doing so would be to lure a user on the remote host into visiting a specially crafted web page.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	24370
CVE	CVE-2007-2219
XREF	MSFT:MS07-035
XREF	IAVA:2007-A-0035
XREF	OSVDB:35341

Ports
tcp/445

```
- C:\WINNT\system32\Kernel32.dll has not been patched
    Remote version : 5.0.2195.6688
    Should be : 5.0.2195.7135
```

24336 - MS07-012: Vulnerability in Microsoft MFC Could Allow Remote Code Execution (924667)

Description

The remote host contains a version of Microsoft Windows that has a vulnerability in the the MFC component that could be abused by an attacker to execute arbitrary code on the remote host.
To exploit this vulnerability, an attacker would need to spend a specially crafted RTF file to a user on the remote host and lure him into opening it.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	22476
CVE	CVE-2007-0025
XREF	MSFT:MS07-012

XREF	OSVDB:31887
XREF	CWE:94

Ports
tcp/445

```
- C:\WINNT\system32\Mfc40u.dll has not been patched
    Remote version : 4.1.0.6140
    Should be : 4.1.0.6141
```

16324 - MS05-008: Vulnerability in Windows Shell (890047)

Description

The remote version of Windows contains a flaw in the Windows Shell that could allow an attacker to elevate his privileges and/or execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to lure a victim into visiting a malicious website or opening a malicious file attachment.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	11466
CVE	CVE-2005-0053
XREF	MSFT:MS05-008
XREF	IAVA:2005-A-0006
XREF	OSVDB:13608

Ports
tcp/445

```
- C:\WINNT\system32\Shell32.dll has not been patched
    Remote version : 5.0.3700.6705
    Should be : 5.0.3900.7009
```

46312 - MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution (978542)

Description

The remote host is running a version of Microsoft Outlook Express / Windows Mail that contains a flaw that could be used to cause an integer overflow, resulting in remote code execution.
To exploit this flaw, an attacker would need a victim to connect to a mail server under their control and send malicious responses to the victim's email client.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	39927
CVE	CVE-2010-0816
XREF	MSFT:MS10-030
XREF	OSVDB:64530

Ports
tcp/445

```
- C:\WINNT\system32\Inetcomm.dll has not been patched
    Remote version : 5.50.4927.1200
    Should be : 5.50.5010.200
```

46839 - MS10-032: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)

Description

The remote Windows host is running a version of the Windows kernel that is affected by one or more of the following vulnerabilities :
- Improper validation of changes in certain kernel objects may allow a local attacker to execute arbitrary code in kernel mode and take complete control of the affected system. (CVE-2010-0484)
- Improper validation of parameters when creating a new window may allow a local attacker to execute arbitrary code in kernel mode and take complete control of the affected system. (CVE-2010-0485)
- A vulnerability that arises in the way Windows provides glyph outline information to applications may allow a local attacker to execute arbitrary code in kernel mode and take complete control of the affected system. (CVE-2010-1255)

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

BID	40570
BID	40569
BID	40508
CVE	CVE-2010-1255
CVE	CVE-2010-0485
CVE	CVE-2010-0484
XREF	MSFT:MS10-032
XREF	IAVA:2010-A-0077
XREF	OSVDB:65225
XREF	OSVDB:65224
XREF	OSVDB:65223

Exploitable with

CANVAS (true)Core Impact (true)

Ports
tcp/445

```
- C:\WINNT\system32\Win32k.sys has not been patched
    Remote version : 5.0.2195.6708
    Should be : 5.0.2195.7397
```

34408 - MS08-063: Microsoft Windows SMB File Name Handling Remote Underflow (957095)

Description

The remote host contains a memory corruption vulnerability in the 'Server' service that may allow an attacker to perform a denial of service against the remote host.

Risk Factor

High

CVSS Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

References

BID	31647
CVE	CVE-2008-4038
XREF	MSFT:MS08-063
XREF	OSVDB:49057
XREF	CWE:119

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\drivers\Srv.sys has not been patched
    Remote version : 5.0.2195.6699
    Should be : 5.0.2195.7177
```

32312 - MS08-028: Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution (950749)

Description

The remote host has a bug in its Microsoft Jet Database Engine (837001).
An attacker may exploit one of these flaws to execute arbitrary code on the remote system.
To exploit this flaw, an attacker would need the ability to craft a specially malformed database query and have this engine execute it.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	26468
BID	12960
CVE	CVE-2007-6026

CVE	CVE-2005-0944
XREF	CWE:119
XREF	MSFT:MS08-028
XREF	IAVA:2008-A-0030
XREF	IAVA:2008-A-0016
XREF	OSVDB:44880
XREF	OSVDB:15187

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\Msjet40.dll has not been patched
    Remote version : 4.0.7328.0
    Should be : 4.0.9511.0
```

46840 - MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)

Description

The remote Windows host has multiple unspecified code execution vulnerabilities related to media decompression. A remote attacker could exploit this by tricking a user into opening a specially crafted media file, resulting in arbitrary code execution.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	40464
BID	40432
CVE	CVE-2010-1880
CVE	CVE-2010-1879
XREF	MSFT:MS10-033
XREF	IAVA:2010-A-0078
XREF	OSVDB:65222
XREF	OSVDB:65221

Ports

tcp/445

```
- C:\WINNT\system32\Asycfilt.dll has not been patched
    Remote version : 2.40.4522.0
    Should be : 2.40.4534.0
```

39341 - MS09-019: Cumulative Security Update for Internet Explorer (969897)

Description

he remote host is missing IE Security Update 969897.
The remote version of IE is affected by several vulnerabilities that may allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	35235
BID	35234
BID	35224
BID	35223
BID	35222
BID	35200
BID	35198
BID	24283
CVE	CVE-2009-1532
CVE	CVE-2009-1531
CVE	CVE-2009-1530
CVE	CVE-2009-1529
CVE	CVE-2009-1528
CVE	CVE-2009-1141
CVE	CVE-2009-1140
CVE	CVE-2007-3091
XREF	CWE:362
XREF	MSFT:MS09-019
XREF	IAVA:2009-A-0045
XREF	OSVDB:54951
XREF	OSVDB:54950
XREF	OSVDB:54949
XREF	OSVDB:54948
XREF	OSVDB:54947

XREF	OSVDB:54946
XREF	OSVDB:54945
XREF	OSVDB:54944
XREF	OSVDB:38497

Ports
tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3877.2200
```

45509 - MS10-022: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169)

Description

The installed version of the VBScript Scripting Engine allows an attacker to specify a Help file location when displaying a dialog box on a web page. If a user can be tricked into pressing the F1 key while such a dialog box is being displayed, an attacker can leverage this to cause the Windows Help System to load a specially crafted Help file, resulting in execution of arbitrary code subject to the user's privileges.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.3 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	38463
CVE	CVE-2010-0483
XREF	CWE:94
XREF	MSFT:MS10-022
XREF	IAVA:2010-A-0056
XREF	OSVDB:62632

Exploitable with

CANVAS (true)Metasploit (true)

Ports
tcp/445

```
- C:\WINNT\system32\Vbscript.dll has not been patched
    Remote version : 5.1.0.7426
    Should be : 5.6.0.8838
```

44416 - MS10-006: Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)

Description

The version of the SMB client software installed on the remote Windows host is affected by two vulnerabilities that could allow arbitrary code execution :
- Improper validation of fields in SMB responses can lead to a pool corruption issue and in turn to arbitrary code execution with SYSTEM level privileges. (CVE-2010-0016)
- Improper handling of a race condition involving SMB 'Negotiate' responses may allow a remote attacker to execute arbitrary code, cause a denial of service, or escalate his privileges. (CVE-2010-0017)

Note that successful exploitation of either issue requires an attacker to trick a user on the affected host into initiating an SMB connection to a malicious SMB server.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	38100
BID	38093
CVE	CVE-2010-0017
CVE	CVE-2010-0016
XREF	CWE:362
XREF	MSFT:MS10-006
XREF	IAVA:2010-A-0032
XREF	OSVDB:62244
XREF	OSVDB:62243

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\drivers\Mrxsmb.sys has not been patched
    Remote version : 5.0.2195.6713
    Should be : 5.0.2195.7362
```

18681 - MS05-036: Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (901214)

Description

The remote host contains a version of the Color Management Module that is vulnerable to a security flaw that could allow an attacker to execute arbitrary code on the remote host by constructing a malicious web page and entice a victim to visit this web page.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	14214
CVE	CVE-2005-1219
XREF	MSFT:MS05-036

XREF	IAVA:2005-A-0018
XREF	OSVDB:17830

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\Mscms.dll has not been patched
    Remote version : 5.0.2180.1
    Should be : 5.0.2195.7054
```

42110 - MS09-054: Cumulative Security Update for Internet Explorer (974455)

Description

The remote host is missing IE Security Update 974455.
The remote version of IE is affected by several vulnerabilities that may allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	36622
BID	36621
BID	36620
BID	36616
CVE	CVE-2009-2531
CVE	CVE-2009-2530
CVE	CVE-2009-2529
CVE	CVE-2009-1547
XREF	CWE:94
XREF	MSFT:MS09-054
XREF	IAVA:2009-A-0093
XREF	OSVDB:58874
XREF	OSVDB:58873
XREF	OSVDB:58872
XREF	OSVDB:58871

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
```

```
    Remote version : 5.0.3700.6699
    Should be : 5.0.3881.100
```

15966 - MS04-041: Vulnerabilities in WordPad (885836)

Description

The remote host contains a version of Microsoft WordPad that is vulnerable to two security flaws.
To exploit these flaws an attacker would need to send a malformed Word file to a victim on the remote host and wait for him to open the file using WordPad.
Opening the file with WordPad will trigger a buffer overflow that could allow an attacker to execute arbitrary code on the remote host with the privileges of the user.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	11929
BID	11927
CVE	CVE-2004-0901
CVE	CVE-2004-0571
XREF	MSFT:MS04-041
XREF	OSVDB:12375
XREF	OSVDB:12373

Ports

tcp/445

```
- C:\Program Files\Windows NT\Accessories\Wordpad.exe has not been patched
    Remote version : 5.0.2170.1
    Should be : 5.0.2195.6991
```

20000 - MS05-047: Vulnerability in Plug and Play Could Allow Remote Code Execution and Local Elevation of Privilege (905749)

Description

The remote host contain a version of the Plug and Play service that contains a vulnerability in the way it handles user-supplied data.
An authenticated attacker could exploit this flaw by sending a malformed RPC request to the remote service and execute code within the SYSTEM context.

Risk Factor

High

CVSS Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

References

BID	15065
CVE	CVE-2005-2120
XREF	MSFT:MS05-047

XREF	OSVDB:18830

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\umpnpmgr.dll has not been patched
    Remote version : 5.0.2182.1
    Should be : 5.0.2195.7069
```

18215 - MS05-024: Vulnerability in Web View Could Allow Code Execution (894320)

Description

The remote host is running a version of Microsoft Windows that contains a security flaw in the Web View of the Windows Explorer that could allow an attacker to execute arbitrary code on the remote host.
To succeed, the attacker would have to send a rogue file to a user of the remote computer and have him preview it using the Web View with the Windows Explorer.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	13248
CVE	CVE-2005-1191
XREF	MSFT:MS05-024
XREF	OSVDB:15707

Ports

tcp/445

```
- C:\WINNT\system32\Webvw.dll has not been patched
    Remote version : 5.0.2920.0
    Should be : 5.0.3900.7036
```

24335 - MS07-011: Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution (926436)

Description

The remote host contains a version of Microsoft Windows that has a vulnerability in the OLE Dialog component that could be abused by an attacker to execute arbitrary code on the remote host.
To exploit this vulnerability, an attacker would need to send a specially crafted RTF file to a user on the remote host and lure him into opening it.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	22483

CVE	CVE-2007-0026
XREF	MSFT:MS07-011
XREF	OSVDB:31885

Ports
tcp/445

```
- C:\WINNT\system32\Oledlg.dll has not been patched
    Remote version : 5.0.2134.1
    Should be : 5.0.2195.7114
```

35075 - MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (959807)

Description

The remote host is running Windows Media Player/Components.
There is a vulnerability in the remote version of this software that may allow an attacker to execute arbitrary code on the remote host thru flaws in ISATAP and SPN.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	32654
BID	32653
CVE	CVE-2008-3010
CVE	CVE-2008-3009
XREF	MSFT:MS08-076
XREF	OSVDB:50559
XREF	OSVDB:50558
XREF	CWE:200

Ports
tcp/445

```
- C:\WINNT\system32\Strmdll.dll has not been patched
    Remote version : 4.1.0.3928
    Should be : 4.1.0.3937
```

26017 - MS07-051: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (938827)

Description

The remote version of Windows contains a flaw in the Microsoft Agent service that may allow an attacker to execute code on the remote host.
To exploit this flaw, an attacker would need to set up a rogue web site and lure a victim on the remote host into visiting it.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	25566
CVE	CVE-2007-3040
XREF	MSFT:MS07-051
XREF	OSVDB:36934
XREF	CWE:119

Exploitable with

CANVAS (true)Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\msagent\Agentdpv.dll has not been patched
    Remote version : 2.0.0.3422
    Should be : 2.0.0.3426
```

39347 - MS09-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)

Description

The remote host contains a version of the Windows kernel that is affected by multiple vulnerabilities :
- A failure of the Windows kernel to properly validate changes in certain kernel objects allows a local user to run arbitrary code in kernel mode. (CVE-2009-1123)
- Insufficient validation of certain pointers passed from user mode allows a local user to run arbitrary code in kernel mode. (CVE-2009-1124)
- A failure to properly validate an argument passed to a Windows kernel system call allows a local user to run arbitrary code in kernel mode. (CVE-2009-1125)
- Improper validation of input passed from user mode to the kernel when editing a specific desktop parameter allows a local user to run arbitrary code in kernel mode. (CVE-2009-1126)

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

BID	35240
BID	35238
BID	35121
BID	35120
CVE	CVE-2009-1126
CVE	CVE-2009-1125
CVE	CVE-2009-1124
CVE	CVE-2009-1123

XREF	MSFT:MS09-025
XREF	OSVDB:54943
XREF	OSVDB:54942
XREF	OSVDB:54941
XREF	OSVDB:54940
XREF	CWE:20

Ports
tcp/445

```
- C:\WINNT\system32\Win32k.sys has not been patched
    Remote version : 5.0.2195.6708
    Should be : 5.0.2195.7279
```

16123 - MS05-001: HTML Help Code Execution (890175)

Description

The remote host contains a version of the HTML Help ActiveX control that could allow an attacker to execute arbitrary code on the remote host by constructing a malicious web page and entice a victim to visit this web page.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2004-1043
XREF	MSFT:MS05-001
XREF	IAVA:2005-A-0002
XREF	OSVDB:12840

Ports
tcp/445

```
- C:\WINNT\system32\Hhctrl.ocx has not been patched
    Remote version : 5.2.3735.1
    Should be : 5.2.3790.233
```

45378 - MS10-018: Cumulative Security Update for Internet Explorer (980182)

Description

The remote host is missing IE Security Update 980182.
The remote version of IE is affected by several vulnerabilities that may allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	39047

BID	39031
BID	39030
BID	39028
BID	39027
BID	39026
BID	39025
BID	39024
BID	39023
BID	38615
CVE	CVE-2010-0807
CVE	CVE-2010-0806
CVE	CVE-2010-0805
CVE	CVE-2010-0494
CVE	CVE-2010-0492
CVE	CVE-2010-0491
CVE	CVE-2010-0490
CVE	CVE-2010-0489
CVE	CVE-2010-0488
CVE	CVE-2010-0267
XREF	MSFT:MS10-018
XREF	IAVA:2010-A-0049
XREF	OSVDB:63335
XREF	OSVDB:63334
XREF	OSVDB:63333
XREF	OSVDB:63332
XREF	OSVDB:63331
XREF	OSVDB:63330
XREF	OSVDB:63329
XREF	OSVDB:63328
XREF	OSVDB:63327
XREF	OSVDB:62810

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports
tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3886.1900
```

15460 - MS04-037: Vulnerability in Windows Shell (841356)

Description

The remote version of Windows contains a flaw in the Windows Shell that could allow an attacker to execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to lure a victim into visiting a malicious website or into opening a malicious file attachment.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	10677
CVE	CVE-2004-0572
CVE	CVE-2004-0214
XREF	MSFT:MS04-037
XREF	IAVA:2004-A-0019
XREF	OSVDB:10699
XREF	OSVDB:10698

Ports
tcp/445

```
- C:\WINNT\system32\Shell32.dll has not been patched
    Remote version : 5.0.3700.6705
    Should be : 5.0.3900.6975
```

20001 - MS05-048: Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution (907245)

Description

An unchecked buffer condition could allow an attacker to execute arbitrary code on the remote host.
To execute this flaw, an attacker would need to send a malformed message via SMTP to the remote host, either by using the SMTP server (if Exchange is installed) or by sending an email to a user on the remote host.
When the email is processed by CDO, an unchecked buffer may allow cause code execution.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.3 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	15067
CVE	CVE-2005-1987
XREF	MSFT:MS05-048
XREF	OSVDB:19905

Ports
tcp/445

```
- C:\WINNT\system32\cdosys.dll has not been patched
    Remote version : 6.1.3940.33
    Should be : 6.1.3940.42
```

18482 - MS05-026: Vulnerability in HTML Help Could Allow Remote Code Execution (896358)

Description

The remote host contains a version of the HTML Help ActiveX control that is vulnerable to a security flaw that could allow an attacker to execute arbitrary code on the remote host by constructing a malicious web page and entice a victim to visit this web page.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	13953
CVE	CVE-2005-1208
XREF	MSFT:MS05-026
XREF	IAVA:2005-A-0017
XREF	OSVDB:17305

Ports
tcp/445

```
- C:\WINNT\system32\Hhctrl.ocx has not been patched
    Remote version : 5.2.3735.1
    Should be : 5.2.3790.309
```

19403 - MS05-040: Vulnerability in Telephony Service Could Allow Remote Code Execution (893756)

Description

The remote host contains a version of the Telephony service that is vulnerable to a security flaw that could allow an attacker to execute arbitrary code and take control of the remote host.
On Windows 2000 and Windows 2003 the server must be enabled and only authenticated user can try to exploit this flaw.
On Windows 2000 Pro and Windows XP this is a local elevation of privilege vulnerability.

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

BID	14518
CVE	CVE-2005-0058
XREF	MSFT:MS05-040
XREF	OSVDB:18606

Exploitable with

CANVAS (true)Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\Tapisrv.dll has not been patched
    Remote version : 5.0.2195.6666
    Should be : 5.0.2195.7057
```

18020 - MS05-016: Vulnerability in Windows Shell (893086)

Description

The remote version of Windows contains a flaw in the Windows Shell that could allow an attacker to elevate his privileges and/or execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to lure a victim into visiting a malicious website or into opening a malicious file attachment.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	13132
CVE	CVE-2005-0063
XREF	MSFT:MS05-016
XREF	IAVA:2005-A-0009
XREF	OSVDB:15469

Ports

tcp/445

```
- C:\WINNT\system32\Shell32.dll has not been patched
    Remote version : 5.0.3700.6705
    Should be : 5.0.3900.7032
```

11878 - MS03-023: Buffer Overrun In HTML Converter Could Allow Code Execution (823559)

Description

The remote host contains a version of the HTML Converter module that could allow an attacker to execute arbitrary code on the remote host by constructing a malicious web page and enticing a victim to visit this web page.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	8016
CVE	CVE-2003-0469
XREF	MSFT:MS03-023
XREF	OSVDB:2963

Ports

tcp/445

```
- C:\Program Files\Common Files\Microsoft Shared\TextConv\Msconv97.dll has not been patched
    Remote version : 1999.9.16.0
    Should be : 2003.1100.5426.0
```

25884 - MS07-046: Vulnerability in GDI Could Allow Remote Code Execution (938829)

Description

The remote host contains a version of Microsoft Windows that has several vulnerabilities in the Graphic Rendering Engine and in the way Windows handles Metafiles.
An attacker may exploit these flaws to execute arbitrary code on the remote host. To exploit this flaw, an attacker would need to send a specially crafted image to a user on the remote host, or lure him into visiting a rogue website containing such a file.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	25302
CVE	CVE-2007-3034
XREF	MSFT:MS07-046
XREF	OSVDB:36388
XREF	CWE:189

Ports

tcp/445

```
- C:\WINNT\system32\gdi32.dll has not been patched
    Remote version : 5.0.2195.6660
    Should be : 5.0.2195.7138
```

33133 - MS08-031: Cumulative Security Update for Internet Explorer (950759)

Description

The remote host is missing the IE cumulative security update 950759.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	29556
BID	28379
CVE	CVE-2008-1544
CVE	CVE-2008-1442
XREF	CWE:20
XREF	MSFT:MS08-031
XREF	IAVA:2008-A-0039
XREF	OSVDB:46084
XREF	OSVDB:46083
XREF	OSVDB:43606

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3864.1800
```

16330 - MS05-015: Vulnerability in the Hyperlink Object Library may allow code execution (888113)

Description

The remote host is running a version of Windows that contains a flaw in the Hyperlink Object Library that can be abused to execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to construct a malicious hyperlink and lure a victim into clicking it.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	12479
CVE	CVE-2005-0057
XREF	MSFT:MS05-015
XREF	OSVDB:13609

Ports

tcp/445

```
- C:\WINNT\system32\Hlink.dll has not been patched
```

```
Remote version : 5.0.0.4513
Should be : 5.2.3790.227
```

35823 - MS09-007: Vulnerability in SChannel Could Allow Spoofing (960225)

Description

The Secure Channel (SChannel) authentication component included in the remote version of Windows does not sufficiently validate certain Transport Layer Security (TLS) handshake messages to ensure that a client does in fact have access to the private key linked to a certificate used for authentication. An attacker who has access to the public key component of a user's certificate may be able to leverage this issue to authenticate as that user against services such as web servers that use certificate-based authentication or to impersonate that user.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	34015
CVE	CVE-2009-0085
XREF	CWE:287
XREF	MSFT:MS09-007
XREF	IAVA:2009-A-0019
XREF	OSVDB:52521

Ports

tcp/445

```
- C:\WINNT\System32\Schannel.dll has not been patched
    Remote version : 5.1.2195.6705
    Should be : 5.1.2195.7213
```

11885 - MS03-045: Buffer Overrun in the ListBox and in the ComboBox (824141)

Description

A vulnerability exists because the ListBox control and the ComboBox control both call a function, located in the User32.dll file, that contains a buffer overrun. A local, interactive attacker could run a program that sends a specially crafted Windows message to any application that has implemented the ListBox control or the ComboBox control, causing the application to take any action he specified.
An attacker must have valid logon credentials to exploit the vulnerability. It can not be exploited remotely.

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8827
CVE	CVE-2003-0659
XREF	MSFT:MS03-045

XREF	IAVA:2005-A-0001
XREF	OSVDB:10938
XREF	OSVDB:10937

Ports
tcp/445

```
- C:\WINNT\system32\User32.dll has not been patched
    Remote version : 5.0.2195.6688
    Should be : 5.0.2195.6799
```

40561 - MS09-042: Vulnerability in Telnet Could Allow Remote Code Execution (960859)

Description

The remote Telnet client does not correctly opt in to NTLM credential- reflection protections, which ensure that a user's credentials are not reflected back and used against the user.
If a remote attacker can trick a user on the host into connecting to a malicious server with an affected version of the Telnet client, he can leverage this issue to gain the rights of that user and do anything that he has privileges to do.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	35993
CVE	CVE-2009-1930
XREF	MSFT:MS09-042
XREF	OSVDB:56904
XREF	CWE:255

Exploitable with

Core Impact (true)

Ports
tcp/445

```
- C:\WINNT\System32\Telnet.exe has not been patched
    Remote version : 5.0.33670.1
    Should be : 5.0.33670.4
```

21210 - MS06-013: Cumulative Security Update for Internet Explorer (912812)

Description

The remote host is missing IE Cumulative Security Update 912812.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	17450
BID	17453
BID	17454
BID	17455
BID	17457
BID	17460
BID	17468
BID	17196
BID	17181
BID	17131
CVE	CVE-2006-1192
CVE	CVE-2006-1191
CVE	CVE-2006-1190
CVE	CVE-2006-1189
CVE	CVE-2006-1188
CVE	CVE-2006-1186
CVE	CVE-2006-1185
CVE	CVE-2006-1388
CVE	CVE-2006-1245
CVE	CVE-2006-1359
XREF	CWE:94
XREF	MSFT:MS06-013
XREF	IAVA:2006-A-0014
XREF	OSVDB:24547
XREF	OSVDB:24546
XREF	OSVDB:24545
XREF	OSVDB:24544
XREF	OSVDB:24543
XREF	OSVDB:24542
XREF	OSVDB:24541

XREF	OSVDB:24095
XREF	OSVDB:24050
XREF	OSVDB:23964

Exploitable with

Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3839.2200
```

43865 - MS10-001: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)

Description

The remote Windows host contains a version of the Embedded OpenType (EOT) Font Engine that is affected by an integer overflow vulnerability in the 'LZCOMP' decompressor when decompressing a specially crafted font.
If an attacker can trick a user on the affected system into viewing content rendered in a specially crafted EOT font, he may be able to leverage this issue to execute arbitrary code subject to the user's privileges.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	37671
CVE	CVE-2010-0018
XREF	CWE:189
XREF	MSFT:MS10-001
XREF	IAVA:2010-A-0003
XREF	OSVDB:61651

Ports

tcp/445

```
- C:\WINNT\System32\T2embed.dll has not been patched
    Remote version : 0.2.0.70
    Should be : 5.0.2195.7348
```

21685 - MS06-021: Cumulative Security Update for Internet Explorer (916281)

Description

The remote host is missing the IE cumulative security update 916281.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	18328
BID	18321
BID	18320
BID	18309
BID	18303
BID	17820
BID	17404
CVE	CVE-2006-2385
CVE	CVE-2006-2384
CVE	CVE-2006-2383
CVE	CVE-2006-2382
CVE	CVE-2006-2218
CVE	CVE-2006-1303
CVE	CVE-2006-1626
XREF	CWE:20
XREF	MSFT:MS06-021
XREF	IAVA:2006-A-0026
XREF	OSVDB:27475
XREF	OSVDB:26446
XREF	OSVDB:26445
XREF	OSVDB:26444
XREF	OSVDB:26443
XREF	OSVDB:26442
XREF	OSVDB:24465

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3841.1900
```

42113 - MS09-057: Vulnerability in Indexing Service Could Allow Remote Code Execution (969059)

Description

The remote host contains the ixsso.dll ActiveX control.
This control is included with the Indexing Service. The version of this control installed on the remote host reportedly has an arbitrary code execution vulnerability. A remote attacker could exploit this by tricking a user into requesting a maliciously crafted web page.
This vulnerability only affects systems that have the Indexing Service enabled. It is disabled by default.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	36629
CVE	CVE-2009-2507
XREF	MSFT:MS09-057
XREF	OSVDB:58854

Ports

tcp/445

```
- C:\WINNT\system32\query.dll has not been patched
    Remote version : 5.0.2195.6664
    Should be : 5.0.2195.7320
```

20002 - MS05-049: Vulnerabilities in Windows Shell Could Allow Remote Code Execution (900725)

Description

The remote version of Windows contains a version of the Windows Shell that has several vulnerabilities. An attacker may exploit these vulnerabilities by :
- Sending a malformed .lnk file a to user on the remote host to trigger an overflow.
- Sending a malformed HTML document to a user on the remote host and have him view it in the Windows Explorer preview pane.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	15064
BID	15069
BID	15070
CVE	CVE-2005-2117
CVE	CVE-2005-2118
CVE	CVE-2005-2122
XREF	MSFT:MS05-049
XREF	IAVA:2005-A-0027

XREF	OSVDB:19900
XREF	OSVDB:19899
XREF	OSVDB:19898

Ports
tcp/445

```
- C:\WINNT\system32\shell32.dll has not been patched
    Remote version : 5.0.3700.6705
    Should be : 5.0.3900.7071
```

35072 - MS08-073: Microsoft Internet Explorer Multiple Vulnerabilities (958215)

Description

The remote host is missing the IE cumulative security update 958215.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	32596
BID	32595
BID	32593
BID	32586
CVE	CVE-2008-4261
CVE	CVE-2008-4260
CVE	CVE-2008-4259
CVE	CVE-2008-4258
XREF	CWE:399
XREF	MSFT:MS08-073
XREF	IAVA:2008-A-0087
XREF	OSVDB:50613
XREF	OSVDB:50612
XREF	OSVDB:50611
XREF	OSVDB:50610

Ports
tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
```

```
    Should be : 5.0.3870.1500
```

11887 - MS03-042: Buffer Overflow in Windows Troubleshooter ActiveX Control (826232)

Description

The remote host contains a version of the Troubleshooter ActiveX control module that could allow an attacker to execute arbitrary code on the remote host by constructing a malicious web page and entice a victim to visit this web page.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	8833
CVE	CVE-2003-0662
XREF	MSFT:MS03-042
XREF	CWE:119
XREF	OSVDB:10999

Ports

tcp/445

```
- C:\WINNT\help\tshoot.ocx has not been patched
    Remote version : 1.0.1.2123
    Should be : 1.0.1.2125
```

44110 - MS10-002: Cumulative Security Update for Internet Explorer (978207)

Description

The remote host is missing IE Security Update 978207.
The remote version of IE is affected by several vulnerabilities that may allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	37895
BID	37894
BID	37893
BID	37892
BID	37891
BID	37884

BID	37883
BID	37815
CVE	CVE-2010-0249
CVE	CVE-2010-0248
CVE	CVE-2010-0247
CVE	CVE-2010-0246
CVE	CVE-2010-0245
CVE	CVE-2010-0244
CVE	CVE-2010-0027
CVE	CVE-2009-4074
XREF	Secunia:38209
XREF	MSFT:MS10-002
XREF	IAVA:2010-A-0029
XREF	IAVA:2010-A-0014
XREF	OSVDB:61914
XREF	OSVDB:61913
XREF	OSVDB:61912
XREF	OSVDB:61911
XREF	OSVDB:61910
XREF	OSVDB:61909
XREF	OSVDB:61697
XREF	OSVDB:60660

Exploitable with

Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3884.1600
```

33135 - MS08-033: Vulnerabilities in DirectX Could Allow Remote Code Execution (951698)

Description

The remote host contains a version of DirectX that is affected by a remote code execution vulnerability.
To exploit this flaw, an attacker would need to send a specially malformed MPEG or SAMI file to a user on the remote host and have him open it.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	29581
BID	29578
CVE	CVE-2008-1444
CVE	CVE-2008-0011
XREF	CWE:119
XREF	MSFT:MS08-033
XREF	IAVA:2008-A-0040
XREF	OSVDB:46065
XREF	OSVDB:46064

Ports

tcp/445

```
- C:\WINNT\system32\quartz.dll has not been patched
    Remote version : 6.1.9.728
    Should be : 6.1.9.734
```

20382 - MS06-001: Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (912919)

Description

The remote host contains a version of Microsoft Windows that is missing a critical security update that fixes several vulnerabilities in the Graphic Rendering Engine, and in the way Windows handles Metafiles.
An attacker could exploit these flaws to execute arbitrary code on the remote host. To exploit this flaw, an attacker would need to send a specially crafted Windows Metafile (WMF) to a user on the remote host, or lure him into visiting a rogue website containing such a file.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	16074
CVE	CVE-2005-4560
XREF	MSFT:MS06-001
XREF	IAVA:2006-A-0001
XREF	OSVDB:21987

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\gdi32.dll has not been patched
    Remote version : 5.0.2195.6660
    Should be : 5.0.2195.7073
```

35221 - MS08-078: Microsoft Internet Explorer Security Update (960714)

Description

The remote host is missing the IE security update 960714.
The remote version of IE is vulnerable to a memory corruption which may allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	32721
CVE	CVE-2008-4844
XREF	CWE:399
XREF	MSFT:MS08-078
XREF	IAVA:2008-A-0090
XREF	OSVDB:50622

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3872.1000
```

36152 - MS09-014: Cumulative Security Update for Internet Explorer (963027)

Description

The remote host is missing IE Security Update 963027.
The remote version of IE is affected by several vulnerabilities that may allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	34438
BID	34426
BID	34424

BID	34423
BID	29445
CVE	CVE-2009-0554
CVE	CVE-2009-0553
CVE	CVE-2009-0552
CVE	CVE-2009-0551
CVE	CVE-2009-0550
CVE	CVE-2008-2540
XREF	CWE:399
XREF	MSFT:MS09-014
XREF	IAVA:2009-A-0035
XREF	IAVA:2009-A-0034
XREF	OSVDB:53627
XREF	OSVDB:53626
XREF	OSVDB:53625
XREF	OSVDB:53624
XREF	OSVDB:53623
XREF	OSVDB:53619

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3874.1900
```

34406 - MS08-061: Microsoft Windows Kernel Multiple Privilege Elevation (954211)

Description

The remote host contains a version of the Windows kernel that is vulnerable to a security flaw that could allow a local user to elevate his privileges or to crash it (therefore causing a denial of service).

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.3 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

BID	31653

BID	31652
BID	31651
CVE	CVE-2008-2252
CVE	CVE-2008-2251
CVE	CVE-2008-2250
XREF	MSFT:MS08-061
XREF	OSVDB:49056
XREF	OSVDB:49055
XREF	OSVDB:49054
XREF	CWE:264

Ports
tcp/445

```
- C:\WINNT\system32\Win32k.sys has not been patched
    Remote version : 5.0.2195.6708
    Should be : 5.0.2195.7194
```

13640 - MS04-022: Task Scheduler Vulnerability (841873)

Description

The remote host is running a version of Windows which contains a flaw in the task scheduler that could lead to arbitrary execution of commands on the remote host.
To exploit this vulnerability, an attacker would need to lure a user on the remote host to take certain steps to execute a .job file, or to visit a rogue web site, then he may be able to execute arbitrary commands on the remote host.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.3 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	10708
CVE	CVE-2004-0212
XREF	MSFT:MS04-022
XREF	IAVA:2004-A-0013
XREF	OSVDB:7798

Ports
tcp/445

```
- C:\WINNT\system32\Mstask.dll has not been patched
    Remote version : 4.71.2195.6704
    Should be : 4.71.2195.6920
```

25881 - MS07-043: Vulnerability in OLE Automation Could Allow Remote Code Execution (921503)

Description

The remote host contains a version of Microsoft Windows that is affected by a vulnerability in the OLE Automation component that could be abused by an attacker to execute arbitrary code on the remote host.
An attacker may be able to execute arbitrary code on the remote host by constructing a malicious script and enticing a victim to visit a web site or view a specially crafted email message.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	25282
CVE	CVE-2007-2224
XREF	CWE:189
XREF	CWE:119
XREF	MSFT:MS07-043
XREF	IAVA:2007-A-0043
XREF	OSVDB:36387

Ports

tcp/445

```
- C:\WINNT\system32\Oleaut32.dll has not been patched
    Remote version : 2.40.4522.0
    Should be : 2.40.4531.0
```

12207 - MS04-014: Microsoft Hotfix (credentialed check) (837001)

Description

The remote host has a bug in its Microsoft Jet Database Engine (837001).
An attacker could exploit one of these flaws to execute arbitrary code on the remote system.
To exploit this flaw, an attacker would need the ability to craft a specially malformed database query and have this engine execute it.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	10112
CVE	CVE-2004-0197
XREF	MSFT:MS04-014
XREF	OSVDB:5241

Ports

tcp/445

```
- C:\WINNT\system32\Msjet40.dll has not been patched
    Remote version : 4.0.7328.0
    Should be : 4.0.8618.0
```

11301 - MS02-040 / MS03-033: Unchecked buffer in MDAC Function (326573 / 823718)

Description

The remote Microsoft Data Access Component (MDAC) server is vulnerable to a flaw that could allow an attacker to execute arbitrary code on this host, provided he can load and execute a database query on this server.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	8455
BID	5372
CVE	CVE-2003-0353
CVE	CVE-2002-0695
XREF	MSFT:MS03-033
XREF	MSFT:MS02-040
XREF	OSVDB:10129
XREF	OSVDB:5135

Ports

tcp/445

```
- C:\WINNT\system32\odbcbcp.dll has not been patched
    Remote version : 3.70.9.61
    Should be : 3.70.11.40
```

16327 - MS05-012: Vulnerability in OLE and COM Could Allow Code Execution (873333)

Description

The remote host is running a version of Windows that is affected by two vulnerabilities when dealing with OLE and/or COM.
These vulnerabilities could allow a local user to escalate his privileges and allow a remote user to execute arbitrary code on the remote host.
To exploit these flaws, an attacker would need to send a specially crafted document to a victim on the remote host.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	12483
BID	12488

CVE	CVE-2005-0044
CVE	CVE-2005-0047
XREF	MSFT:MS05-012
XREF	IAVA:2005-A-0007
XREF	OSVDB:13602
XREF	OSVDB:13601

Ports
tcp/445

```
- C:\WINNT\system32\Ole32.dll has not been patched
    Remote version : 5.0.2195.6692
    Should be : 5.0.2195.7021
```

25025 - MS07-022: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784)

Description
The remote host contains a version of the Windows kernel that is vulnerable to a security flaw which could allow a local user to elevate his privileges or to crash it (therefore causing a denial of service).

Risk Factor
High

CVSS Base Score
7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score
5.3 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

BID	23367
CVE	CVE-2007-1206
XREF	MSFT:MS07-022
XREF	OSVDB:34011

Ports
tcp/445

```
- C:\WINNT\System32\Ntoskrnl.exe has not been patched
    Remote version : 5.0.2195.6717
    Should be : 5.0.2195.7133
```

31042 - MS08-008: Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)

Description
The remote host contains a version of Microsoft Windows that has a vulnerability in the OLE Automation component that can be abused by an attacker to execute arbitrary code on the remote host.
An attacker may be able to execute arbitrary code on the remote host by constructing a malicious script and enticing a victim to visit a web site or view a specially-crafted email message.

Risk Factor
High

CVSS Base Score
9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	27661
CVE	CVE-2007-0065
XREF	CWE:94
XREF	MSFT:MS08-008
XREF	IAVA:2008-A-0006
XREF	OSVDB:41463

Ports

tcp/445

```
- C:\WINNT\system32\Oleaut32.dll has not been patched
    Remote version : 2.40.4522.0
    Should be : 2.40.4532.0
```

39792 - MS09-029: Vulnerabilities in the Embedded OpenType Font Engine Could Allow Remote Code Execution (961371)

Description

The remote Windows host contains a version of the Embedded OpenType (EOT) Font Engine that is affected by multiple buffer overflow vulnerabilities due to the way the EOT font technology parses name tables in specially crafted embedded fonts.
If an attacker can trick a user on the affected system into viewing content rendered in a specially crafted EOT font, he may be able to leverage these issues to execute arbitrary code subject to the user's privileges.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	35187
BID	35186
CVE	CVE-2009-0232
CVE	CVE-2009-0231
XREF	CWE:189
XREF	MSFT:MS09-029
XREF	IAVA:2009-A-0052
XREF	OSVDB:55843
XREF	OSVDB:55842

Ports

tcp/445

```
- C:\WINNT\System32\T2embed.dll has not been patched
    Remote version : 0.2.0.70
```

```
    Should be : 5.0.2195.7263
```

15963 - MS04-044: Vulnerabilities in Windows Kernel and LSASS (885835)

Description

The remote host is running version of the NT kernel and LSASS which could allow a local user to gain elevated privileged.
An attacker who has the ability to execute arbitrary commands on the remote host could exploit these flaws to gain SYSTEM privileges.

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

BID	11914
BID	11913
CVE	CVE-2004-0894
CVE	CVE-2004-0893
XREF	MSFT:MS04-044
XREF	OSVDB:12376
XREF	OSVDB:12372

Exploitable with

CANVAS (true)

Ports

tcp/445

```
- C:\WINNT\system32\Lsasrv.dll has not been patched
    Remote version : 5.0.2195.6695
    Should be : 5.0.2195.6987
```

33878 - MS08-049: Vulnerabilities in Event System Could Allow Remote Code Execution (950974)

Description

The remote version of Windows contains a vulnerability in the Event System that might allow an attacker to execute arbitrary code on the remote host.
To exploit this vulnerability, an attacker with valid logon credentials would need to send a malformed subscription request to the remote Event System.

Risk Factor

High

CVSS Base Score

8.5 (CVSS2#AV:N/AC:M/Au:S/C:C/I:C/A:C)

References

BID	30586
BID	30584
CVE	CVE-2008-1456
CVE	CVE-2008-1457
XREF	CWE:20

XREF	MSFT:MS08-049
XREF	OSVDB:47412
XREF	OSVDB:47411

Exploitable with

CANVAS (true)

Ports

tcp/445

```
- C:\WINNT\system32\es.dll has not been patched
    Remote version : 2000.2.3504.0
    Should be : 2000.2.3550.0
```

20172 - MS05-053: Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (896424)

Description

The remote host contains a version of Microsoft Windows missing a critical security update to fix several vulnerabilities in the Graphic Rendering Engine, and in the way Windows handles Metafiles.
An attacker could exploit these flaws to execute arbitrary code on the remote host by sending a specially crafted Windows Metafile (WMF) or Enhanced Metafile (EMF) to a victim on the remote host. When viewing the malformed file, a buffer overflow condition occurs that may allow the execution of arbitrary code with the privileges of the user.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

BID	15356
BID	15352
CVE	CVE-2005-0803
CVE	CVE-2005-2124
CVE	CVE-2005-2123
XREF	MSFT:MS05-053
XREF	IAVA:2005-A-0039
XREF	OSVDB:20580
XREF	OSVDB:20579
XREF	OSVDB:18820
XREF	OSVDB:14862

Exploitable with

Metasploit (true)

Ports

tcp/445

```
- C:\WINNT\system32\gdi32.dll has not been patched
    Remote version : 5.0.2195.6660
    Should be : 5.0.2195.7069
```

15457 - MS04-032: Security Update for Microsoft Windows (840987)

Description

The remote host is missing a security update for Microsoft Windows (840987). The missing security update fixes issues in the following areas :
- Window Management
- Virtual DOS Machine
- Graphics Rendering Engine
- Windows Kernel
A local attacker could exploit any of these vulnerabilities to cause a local denial of service or obtain higher privileges on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	11378
BID	11375
BID	11369
BID	11365
CVE	CVE-2004-0211
CVE	CVE-2004-0209
CVE	CVE-2004-0208
CVE	CVE-2004-0207
XREF	MSFT:MS04-032
XREF	IAVA:2004-A-0017
XREF	OSVDB:10693
XREF	OSVDB:10692
XREF	OSVDB:10691
XREF	OSVDB:10690

Ports

tcp/445

```
- C:\WINNT\system32\Win32k.sys has not been patched
    Remote version : 5.0.2195.6708
    Should be : 5.0.2195.6966
```

21331 - MS06-018: Vulnerability in MSDTC Could Allow Denial of Service (913580)

Description

The remote version of Windows contains a version of MSDTC that contains several denial of service vulnerabilities (DoS and Invalid Memory Access).
An attacker may exploit these flaws to crash the remote service.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	17906
BID	17905
CVE	CVE-2006-0034
CVE	CVE-2006-1184
XREF	MSFT:MS06-018
XREF	OSVDB:25336
XREF	OSVDB:25335

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\Msdtctm.dll has not been patched
    Remote version : 2000.2.3504.0
    Should be : 2000.2.3535.0
```

20389 - MS06-002: Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution (908519)

Description

The remote version of Microsoft Windows contains a flaw in the Embedded Web Font engine. An attacker could execute arbitrary code on the remote host by constructing a malicious web page and entice a victim to visit this web page or by sending a malicious font file.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	16194
CVE	CVE-2006-0010
XREF	CWE:119
XREF	MSFT:MS06-002
XREF	IAVA:2006-A-0002
XREF	OSVDB:18829

Ports

tcp/445

```
- C:\WINNT\system32\Fontsub.dll has not been patched
    Remote version : 5.0.2180.1
```

```
    Should be : 5.0.2195.7071
```

26962 - MS07-056: Cumulative Security Update for Outlook Express and Windows Mail (941202)

Description

The remote host is running a version of Microsoft Outlook Express that contains several security flaws that could allow an attacker to execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to send a malformed email to a victim on the remote host and have him open it.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	25908
CVE	CVE-2007-3897
XREF	MSFT:MS07-056
XREF	OSVDB:37631
XREF	CWE:119

Ports

tcp/445

```
- C:\WINNT\system32\Inetcomm.dll has not been patched
    Remote version : 5.50.4927.1200
    Should be : 5.50.4980.1600
```

34403 - MS08-058: Microsoft Internet Explorer Multiple Vulnerabilities (956390)

Description

The remote host is missing the IE cumulative security update 956390.
The remote version of IE is vulnerable to several flaws that could allow an attacker to execute arbitrary code on the remote host.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	31654
BID	31618
BID	31617
BID	31616
BID	31615
BID	29960

CVE	CVE-2008-3476
CVE	CVE-2008-3475
CVE	CVE-2008-3474
CVE	CVE-2008-3473
CVE	CVE-2008-3472
CVE	CVE-2008-2947
XREF	CWE:399
XREF	MSFT:MS08-058
XREF	IAVA:2008-A-0079
XREF	OSVDB:49118
XREF	OSVDB:49117
XREF	OSVDB:49116
XREF	OSVDB:49115
XREF	OSVDB:49114
XREF	OSVDB:49113
XREF	OSVDB:46630

Ports
tcp/445

```
- C:\WINNT\system32\Mshtml.dll has not been patched
    Remote version : 5.0.3700.6699
    Should be : 5.0.3868.2000
```

16329 - MS05-013: Vulnerability in the DHTML Editing Component may allow code execution (891781)

Description

The remote host is running a version of Windows which contains a flaw in the DHTML Editing Component ActiveX Control.
An attacker could exploit this flaw to execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to construct a malicious web page and lure a victim into visiting it.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	11950
CVE	CVE-2004-1319
XREF	MSFT:MS05-013
XREF	OSVDB:12424

Ports
tcp/445

```
- C:\Program Files\Common Files\Microsoft Shared\Triedit\Dhtmled.ocx has not been patched
    Remote version : 6.1.0.8594
    Should be : 6.1.0.9232
```

20003 - MS05-050: Vulnerability in DirectShow Could Allow Remote Code Execution (904706)

Description

The remote host contains a version of DirectX that is vulnerable to a remote code execution flaw.
To exploit this flaw, an attacker would need to send a specially malformed .avi file to a user on the remote host and have him open it.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	15063
CVE	CVE-2005-2128
XREF	MSFT:MS05-050
XREF	IAVA:2005-A-0029
XREF	OSVDB:18822

Ports
tcp/445

```
- C:\WINNT\system32\quartz.dll has not been patched
    Remote version : 6.1.9.728
    Should be : 6.1.9.732
```

25024 - MS07-021: Vulnerabilities in CSRSS Could Allow Remote Code Execution (930178)

Description

The remote host is running a version of Windows containing a bug in the CSRSS error message handling routine that could allow an attacker to execute arbitrary code on the remote host by luring a user on the remote host into visiting a rogue web site.
Additionally, the system is prone to the following types of attack :
- Local Priviledge Elevation
- Denial of Service (Local)

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	23338
BID	23324
BID	21688
CVE	CVE-2007-1209

CVE	CVE-2006-6797
CVE	CVE-2006-6696
XREF	MSFT:MS07-021
XREF	OSVDB:34008
XREF	OSVDB:31897
XREF	OSVDB:31659
XREF	CWE:119

Exploitable with

CANVAS (true)

Ports

tcp/445

```
- C:\WINNT\System32\Winsrv.dll has not been patched
    Remote version : 5.0.2195.6699
    Should be : 5.0.2195.7135
```

22192 - MS06-050: Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution (920670)

Description

The remote host is running a version of Windows that contains a flaw in the Hyperlink Object Library.
An attacker could exploit this flaw to execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to construct a malicious hyperlink and lure a victim into clicking it.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	19405
CVE	CVE-2006-3438
CVE	CVE-2006-3086
XREF	MSFT:MS06-050
XREF	OSVDB:29724
XREF	OSVDB:26666
XREF	CWE:119

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\Hlink.dll has not been patched
    Remote version : 5.0.0.4513
    Should be : 5.2.3790.2748
```

40888 - MS09-045: Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution (971961)

Description

The remote host is running a version of Windows that contains a flaw in its JScript scripting engine.
An attacker may be able to execute arbitrary code on the remote host by constructing a malicious JScript and enticing a victim to visit a web site or view a specially crafted email message.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	36224
CVE	CVE-2009-1920
XREF	CWE:94
XREF	MSFT:MS09-045
XREF	IAVA:2009-A-0074
XREF	OSVDB:57804

Ports

tcp/445

```
- C:\WINNT\System32\Jscript.dll has not been patched
    Remote version : 5.1.0.8513
    Should be : 5.6.0.8837
```

45507 - MS10-020: Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)

Description

The version of the SMB client software installed on the remote Windows host may be affected by one or more vulnerabilities, including some that could allow arbitrary code execution :
- Incorrect handling of incomplete SMB responses could be abused to cause the system to stop responding. (CVE-2009-3676)
- A vulnerability in the way the SMB client allocates memory when parsing specially crafted SMB responses could be abused by an unauthenticated, remote attacker to execute arbitrary code with system-level privileges. (CVE-2010-0269)
- Improper validation of fields in SMB responses could lead to a memory corruption issue and in turn to arbitrary code execution with system-level privileges. (CVE-2010-0270)
- Improper parsing of SMB transaction responses could lead to a memory corruption issue resulting in code execution with system-level privileges. (CVE-2010-0476)
- Improper handling of SMB responses could cause the SMB client to consume the entire response and indicate an invalid value to the Winsock kernel, which in turn could allow remote code execution and result in the compromise of the affected system. (CVE-2010-0477)

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

BID	39340

BID	39339
BID	39336
BID	39312
BID	36989
CVE	CVE-2010-0477
CVE	CVE-2010-0476
CVE	CVE-2010-0270
CVE	CVE-2010-0269
CVE	CVE-2009-3676
XREF	MSFT:MS10-020
XREF	IAVA:2010-A-0055
XREF	OSVDB:64928
XREF	OSVDB:64927
XREF	OSVDB:64926
XREF	OSVDB:64925
XREF	OSVDB:59957

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\drivers\Mrxsmb.sys has not been patched
    Remote version : 5.0.2195.6713
    Should be : 5.0.2195.7379
```

22034 - MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)

Description

The remote host is vulnerable to heap overflow in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.
In addition to this, the remote host is also affected by an information disclosure vulnerability in SMB that may allow an attacker to obtain portions of the memory of the remote host.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	18891
BID	18863

CVE	CVE-2006-1315
CVE	CVE-2006-1314
XREF	MSFT:MS06-035
XREF	OSVDB:27155
XREF	OSVDB:27154

Exploitable with

Core Impact (true)

Ports

tcp/445

39622 - MS09-032: Cumulative Security Update of ActiveX Kill Bits (973346)

Description

The remote host is missing a list of kill bits for ActiveX controls that are known to contain vulnerabilities.
If these ActiveX controls are ever installed on the remote host, either now or in the future, they would expose it to various security issues.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

4.2 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

BID	35558
CVE	CVE-2008-0015
XREF	CWE:119
XREF	MSFT:MS09-032
XREF	IAVA:2009-A-0067
XREF	IAVA:2009-A-0051
XREF	OSVDB:55651

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
The kill bit has not been set for the following control :

  {011B3619-FE63-4814-8A84-15A194CE9CE3}

Note that Nessus did not check whether there were other kill bits
that have not been set because 'Thorough tests' was not enabled
when this scan was run.
```

43061 - MS09-069: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (974392)

Description

The version of LSASS running on the remote host improperly handles specially crafted ISAKMP messages communicated through IPsec, causing the system to consume excessive amounts of CPU resources. A remote, authenticated attacker could exploit this to cause a denial of service.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:C)

CVSS Temporal Score

5.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:C)

References

BID	37218
CVE	CVE-2009-3675
XREF	MSFT:MS09-069
XREF	OSVDB:60831
XREF	CWE:399

Ports

tcp/445

```
- C:\WINNT\system32\Oakley.dll has not been patched
    Remote version : 5.0.2195.6662
    Should be : 5.0.2195.7343
```

18485 - MS05-032: Vulnerability in Microsoft Agent Could Allow Spoofing (890046)

Description

The remote version of Windows contains a flaw in the Microsoft Agent service that could allow an attacker to spoof the content of a web site.
To exploit this flaw, an attacker would need to set up a rogue web site and lure a victim on the remote host into visiting it.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.2 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

BID	13948
CVE	CVE-2005-1214
XREF	MSFT:MS05-032
XREF	OSVDB:17310

Ports

tcp/445

```
- C:\WINNT\msagent\Agentdpv.dll has not been patched
    Remote version : 2.0.0.3422
    Should be : 2.0.0.3423
```

44418 - MS10-008: Cumulative Security Update of ActiveX Kill Bits (978262)

Description

The Microsoft Data Analyzer ActiveX control has a remote code execution vulnerability. The system may also have one or more vulnerable third-party ActiveX controls installed.

A remote attacker could exploit these issues by tricking a user into requesting a maliciously crafted web page, resulting in arbitrary code execution.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

4.4 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

BID	38067
BID	38066
BID	38060
BID	38045
BID	34766
CVE	CVE-2010-0252
CVE	CVE-2009-3735
CVE	CVE-2009-2570
XREF	CWE:94
XREF	MSFT:MS10-008
XREF	IAVA:2010-A-0074
XREF	IAVA:2010-A-0023
XREF	OSVDB:62438
XREF	OSVDB:62372
XREF	OSVDB:62267
XREF	OSVDB:62246
XREF	OSVDB:54137

Exploitable with

Core Impact (true)

Ports

tcp/445

```
{E0ECA9C3-D669-4EF4-8231-00724ED9288F}
```

21211 - MS06-014: Vulnerability in MDAC Could Allow Code Execution (911562)

Description

The remote Microsoft Data Access Component (MDAC) server is vulnerable to a flaw that could allow a local administrator to elevate his privileges to the 'system' level, thus gaining the complete control over the remote system.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

4.2 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

BID	17462
CVE	CVE-2006-0003
XREF	MSFT:MS06-014
XREF	OSVDB:24517

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

```
- C:\Program Files\Common Files\system\msadc\\msadco.dll has not been patched
    Remote version : 2.53.6202.0
    Should be : 2.53.6306.0
```

33877 - MS08-048: Security Update for Outlook Express and Windows Mail (951066)

Description

The remote host is running a version of Microsoft Outlook Express which contains a flaw that might be used to cause an information disclosure.
To exploit this flaw, an attacker would need to send a malformed email to a victim on the remote host and have him open it.

Risk Factor

Medium

CVSS Base Score

5.4 (CVSS2#AV:N/AC:H/Au:N/C:C/I:N/A:N)

CVSS Temporal Score

4.5 (CVSS2#AV:N/AC:H/Au:N/C:C/I:N/A:N)

References

BID	30585
CVE	CVE-2008-1448
XREF	MSFT:MS08-048
XREF	OSVDB:47413
XREF	CWE:264

Ports

tcp/445

```
- C:\WINNT\system32\Inetcomm.dll has not been patched
    Remote version : 5.50.4927.1200
    Should be : 5.50.4990.2500
```

42112 - MS09-056: Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571)

Description

The remote Windows host contains a version of the Microsoft Windows CryptoAPI that is affected by multiple vulnerabilities :

- A spoofing vulnerability exists in the Microsoft Windows CryptoAPI component when parsing ASN.1 information from X.509 certificates. An attacker who successfully exploited this vulnerability could impersonate another user or system. (CVE-2009-2510)
- A spoofing vulnerability exists in the Microsoft Windows CryptoAPI component when parsing ASN.1 object identifiers from X.509 certificates. An attacker who successfully exploited this vulnerability could impersonate another user or system. (CVE-2009-2511)

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.1 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	36577
BID	36475
CVE	CVE-2009-2511
CVE	CVE-2009-2510
XREF	CWE:189
XREF	MSFT:MS09-056
XREF	IAVA:2009-A-0095
XREF	OSVDB:58856
XREF	OSVDB:58855

Ports

tcp/445

```
- C:\WINNT\system32\msasn1.dll has not been patched
    Remote version : 5.0.2195.6666
    Should be : 5.0.2195.7334
```

22187 - MS06-045: Vulnerability in Windows Explorer Could Allow Remote Code Execution (921398)

Description

The remote host is running a version of Windows that contains a flaw in the Windows Explorer Drag & Drop handler. An attacker may be able to execute arbitrary code on the remote host by constructing a malicious script and enticing a victim to visit a web site or view a specially-crafted email message and save a file.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

4.2 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

BID	19389
CVE	CVE-2006-3281
XREF	MSFT:MS06-045

XREF	IAVA:2006-A-0038
XREF	OSVDB:26957

Ports
tcp/445

```
- C:\WINNT\system32\Shell32.dll has not been patched
    Remote version : 5.0.3700.6705
    Should be : 5.0.3900.7105
```

21212 - MS06-015: Vulnerabilities in Windows Explorer Could Allow Remote Code Execution (908531)

Description

The remote version of Windows contains a version of the Windows Explorer that has a vulnerability in the way it handles COM objects.
An attacker could exploit this vulnerability by asking a victim to visit a rogue website containing a malformed COM object.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

3.8 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

BID	17464
CVE	CVE-2006-0012
XREF	MSFT:MS06-015
XREF	IAVA:2006-A-0015
XREF	OSVDB:24516

Ports
tcp/445

```
- C:\WINNT\system32\shell32.dll has not been patched
    Remote version : 5.0.3700.6705
    Should be : 5.0.3900.7078
```

42111 - MS09-055: Cumulative Security Update of ActiveX Kill Bits (973525)

Description

Microsoft ActiveX controls that were compiled using the vulnerable Active Template Library described in Microsoft Security Bulletin MS09-035 have remote code execution vulnerabilities. A remote attacker could exploit them to execute arbitrary code by tricking a user into requesting a maliciously crafted web page.

See Also

http://technet.microsoft.com/en-us/security/bulletin/MS09-035

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

3.8 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

BID	35828
CVE	CVE-2009-2493
XREF	CWE:264
XREF	MSFT:MS09-055
XREF	MSFT:MS09-035
XREF	IAVA:2009-A-0127
XREF	IAVA:2009-A-0097
XREF	IAVA:2009-A-0094
XREF	IAVA:2009-A-0067
XREF	IAVA:2009-A-0063
XREF	IAVA:2009-A-0061
XREF	OSVDB:56698

Ports
tcp/445

```
The kill bit has not been set for the following control :

  {0002E531-0000-0000-C000-000000000046}

Note that Nessus did not check whether there were other kill bits
that have not been set because 'Thorough tests' was not enabled
when this scan was run.
```

33134 - MS08-032: Cumulative Security Update of ActiveX Kill Bits (950760)

Description
The remote host contains the sapi.dll ActiveX control.
The version of this control installed on the remote host reportedly contains multiple memory corruption flaws. If an attacker can trick a user on the affected host into visiting a specially crafted web page, he may be able to leverage this issue to execute arbitrary code on the host subject to the user's privileges.

Risk Factor
Medium

CVSS Base Score
5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score
3.8 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References
BID	29558
CVE	CVE-2008-0956
CVE	CVE-2007-0675
XREF	CWE:119
XREF	MSFT:MS08-032
XREF	OSVDB:46087

XREF	OSVDB:46076
XREF	OSVDB:46062
XREF	OSVDB:33627

Ports
tcp/445

```
The kill bit has not been set for the following control :

  {47206204-5eca-11d2-960f-00c04f8ee628}

Note that Nessus did not check whether there were other kill bits
that have not been set because 'Thorough tests' was not enabled
when this scan was run.
```

22186 - MS06-044: Vulnerability in Microsoft Management Console Could Allow Remote Code Execution (917008)

Description
The remote host is running a version of Windows that contains a flaw in the Management Console.
An attacker may be able to execute arbitrary code on the remote host by constructing a malicious script and enticing a victim to visit a web site or view a specially crafted email message.

Risk Factor
Medium

CVSS Base Score
6.0 (CVSS2#AV:N/AC:M/Au:S/C:P/I:P/A:P)

CVSS Temporal Score
5.0 (CVSS2#AV:N/AC:M/Au:S/C:P/I:P/A:P)

References
BID	19417
CVE	CVE-2006-3643
XREF	MSFT:MS06-044
XREF	OSVDB:27842
XREF	CWE:79

Ports
tcp/445

```
- C:\WINNT\system32\Mmcndmgr.dll has not been patched
    Remote version : 5.0.2195.6601
    Should be : 5.0.2195.7102
```

21213 - MS06-016: Vulnerability in Outlook Express Could Allow Remote Code Execution (911567)

Description
The remote host is running a version of Microsoft Outlook Express that may allow an attacker to execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to send a malformed Windows Address Book (.wab) file to a victim on the remote host and have him open the file.

Risk Factor
Medium

CVSS Base Score
5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

3.8 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

BID	17459
CVE	CVE-2006-0014
XREF	MSFT:MS06-016
XREF	IAVA:2006-A-0016
XREF	OSVDB:24519

Ports

tcp/445

```
- C:\Program Files\Outlook Express\\msoe.dll has not been patched
    Remote version : 5.50.4927.1200
    Should be : 5.50.4963.1700
```

44421 - MS10-011: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (978037)

Description

The remote host allows elevation of privileges in its Windows Client/Server run-time subsystem (CSRSS) because of a failure to properly terminate user processes when a user logs out.
An attacker might exploit this to run arbitrary code in kernel mode.

Risk Factor

Medium

CVSS Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.1 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

References

BID	38098
CVE	CVE-2010-0023
XREF	CWE:264
XREF	MSFT:MS10-011
XREF	IAVA:2010-A-0024
XREF	OSVDB:62252

Ports

tcp/445

```
- C:\WINNT\system32\Csrsrv.dll has not been patched
    Remote version : 5.0.2195.6601
    Should be : 5.0.2195.7366
```

31039 - MS08-005: Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831)

Description

The remote host contains a version of Microsoft Internet Information Services (IIS) that is vulnerable to a security flaw that could allow a local user to elevate his privileges to SYSTEM due to a bug in the way IIS handles file change notifications in the FTPRoot, NNTPFile\Root and WWWRoot folders.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS Temporal Score

5.0 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

References

BID	27101
CVE	CVE-2008-0074
XREF	MSFT:MS08-005
XREF	OSVDB:41456
XREF	CWE:264

Ports

tcp/445

```
- C:\WINNT\system32\inetsrv\infocomm.dll has not been patched
    Remote version : 5.0.2195.6709
    Should be : 5.0.2195.7147
```

12267 - MS04-016: Vulnerability in DirectPlay Could Allow Denial of Service (839643)

Description

The remote host contains a version of version of DirectPlay that is vulnerable to a denial of service attack. DirectPlay is a component of DirectX and is frequently used by game developpers to create networked multi-player games. An attacker could exploit this flaw by sending a malformed IDirectPlay packet to a remote application using this service and cause it to crash.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

BID	10487
CVE	CVE-2004-0202
XREF	MSFT:MS04-016
XREF	OSVDB:6742

Ports

tcp/445

```
- C:\WINNT\system32\Dplayx.dll has not been patched
    Remote version : 5.0.2169.1
    Should be : 5.0.2195.6922
```

46841 - MS10-034: Cumulative Security Update of ActiveX Kill Bits (980195)

Description

The Microsoft Data Analyzer ActiveX control has a remote code execution vulnerability. The system may also have one or more vulnerable third-party ActiveX controls installed.

A remote attacker could exploit these issues by tricking a user into requesting a maliciously crafted web page, resulting in arbitrary code execution.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

3.8 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

BID	40535
BID	40496
BID	40494
BID	40490
BID	38045
CVE	CVE-2010-2193
CVE	CVE-2010-0811
CVE	CVE-2010-0252
XREF	CWE:94
XREF	MSFT:MS10-034
XREF	IAVA:2011-A-0038
XREF	IAVA:2010-A-0074
XREF	IAVA:2010-A-0023
XREF	OSVDB:65481
XREF	OSVDB:65480
XREF	OSVDB:65468
XREF	OSVDB:65382
XREF	OSVDB:65218
XREF	OSVDB:62246

Ports

tcp/445

```
The kill bit has not been set for the following control :

  {14FD1463-1F3F-4357-9C03-2080B442F503}

Note that Nessus did not check whether there were other kill bits
that have not been set because "Thorough tests" was not enabled
when this scan was run.
```

46844 - MS10-037: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege (980218)

Description

The remote Windows host contains a version of the OpenType Compact Font Format (CFF) Font Driver that fails to properly validate certain data passed from user mode to kernel mode.
By viewing content rendered in a specially crafted CFF font, a local attacker may be able to exploit this vulnerability to execute arbitrary code in kernel mode and take complete control of the affected system.

Risk Factor

Medium

CVSS Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.1 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

References

BID	40572
CVE	CVE-2010-0819
XREF	MSFT:MS10-037
XREF	OSVDB:65217

Ports

tcp/445

```
- C:\WINNT\System32\Atmfd.dll has not been patched
    Remote version : 5.0.2.225
    Should be : 5.0.2.227
```

44425 - MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165)

Description

The remote Windows host is running a version of the Windows kernel that is affected by two vulnerabilities :
- An elevation of privilege vulnerability exists in the kernel due to the way it handles certain exceptions. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs, view / change / delete data, or create new accounts with full user rights.
(CVE-2010-0232)
- An elevation of privilege vulnerability exists in the Windows kernel due to a double free condition. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs, view / change / delete data, or create new accounts with full user rights.
(CVE-2010-0233)

Risk Factor

Medium

CVSS Base Score

6.2 (CVSS2#AV:L/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.1 (CVSS2#AV:L/AC:H/Au:N/C:C/I:C/A:C)

References

BID	38044
BID	37864
CVE	CVE-2010-0232
CVE	CVE-2010-0233
XREF	CWE:20
XREF	MSFT:MS10-015

XREF	IAVA:2010-A-0026
XREF	OSVDB:62259
XREF	OSVDB:61854

Exploitable with

CANVAS (true)Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\ntoskrnl.exe has not been patched
    Remote version : 5.0.2195.6717
    Should be : 5.0.2195.7364
```

31793 - MS08-020: Vulnerability in DNS Client Could Allow Spoofing (945553)

Description

There is a flaw in the remote DNS client that could let an attacker send malicious DNS responses to DNS requests made by the remote host, thereby spoofing or redirecting internet traffic from legitimate locations.

Risk Factor

Medium

CVSS Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSS Temporal Score

4.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

References

BID	28553
CVE	CVE-2008-0087
XREF	MSFT:MS08-020
XREF	OSVDB:44172
XREF	CWE:287

Ports

tcp/445

```
- C:\WINNT\system32\dnsapi.dll has not been patched
    Remote version : 5.0.2195.6680
    Should be : 5.0.2195.7151
```

33441 - MS08-037: Vulnerabilities in DNS Could Allow Spoofing (953230)

Description

Flaws in the remote DNS library may let an attacker send malicious DNS responses to DNS requests made by the remote host, thereby spoofing or redirecting internet traffic from legitimate locations.

Risk Factor

Medium

CVSS Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSS Temporal Score

4.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

References

BID	30132
BID	30131
CVE	CVE-2008-1454
CVE	CVE-2008-1447
XREF	MSFT:MS08-037
XREF	IAVA:2008-A-0055
XREF	IAVA:2008-A-0045
XREF	IAVA:2008-A-0044
XREF	OSVDB:46778
XREF	OSVDB:46777

Ports
tcp/445

```
- C:\WINNT\system32\dnsapi.dll has not been patched
    Remote version : 5.0.2195.6680
    Should be : 5.0.2195.7280
```

11990 - MS04-003: MDAC Buffer Overflow (832483)

Description

The remote Microsoft Data Access Component (MDAC) server is vulnerable to a flaw that could allow an attacker to execute arbitrary code on this host, provided he can simulate responses from a SQL server.
To exploit this flaw, an attacker would need to wait for a host running a vulnerable MDAC implementation to send a broadcast query. He would then need to send a malicious packet pretending to come from a SQL server.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:A/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.0 (CVSS2#AV:A/AC:H/Au:N/C:C/I:C/A:C)

References

BID	9407
CVE	CVE-2003-0903
XREF	MSFT:MS04-003
XREF	CWE:119
XREF	OSVDB:3457

Ports
tcp/445

```
- C:\WINNT\system32\odbcbcp.dll has not been patched
    Remote version : 3.70.9.61
    Should be : 3.70.11.46
```

21687 - MS06-023: Vulnerability in Microsoft JScript Could Allow Remote Code Execution (917344)

Description

The remote host is running a version of Windows that contains a flaw in JScript.
An attacker may be able to execute arbitrary code on the remote host by constructing a malicious JScript and enticing a victim to visit a web site or view a specially crafted email message.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.0 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

References

BID	18359
CVE	CVE-2006-1313
XREF	MSFT:MS06-023
XREF	OSVDB:26434

Ports

tcp/445

```
- C:\WINNT\system32\Jscript.dll has not been patched
    Remote version : 5.1.0.8513
    Should be : 5.1.0.12512
```

45511 - MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832)

Description

The installed version of Microsoft Exchange / Windows SMTP Service is affected by at least one vulnerability :
- Incorrect parsing of DNS Mail Exchanger (MX) resource records could cause the Windows Simple Mail Transfer Protocol (SMTP) component to stop responding until the service is restarted. (CVE-2010-0024)
- Improper allocation of memory for interpreting SMTP command responses may allow an attacker to read random e-mail message fragments stored on the affected server.
(CVE-2010-0025)
- Predictable transaction IDs are used, which could allow a man-in-the-middle attacker to spoof DNS responses.
(CVE-2010-1689)
- There is no verification that the transaction ID of a response matches the transaction ID of a query, which could allow a man-in-the-middle attacker to spoof DNS responses. (CVE-2010-1690)

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:P)

CVSS Temporal Score

5.3 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:P)

References

BID	39910
BID	39908
BID	39381
BID	39308
CVE	CVE-2010-1690
CVE	CVE-2010-1689

CVE	CVE-2010-0025
CVE	CVE-2010-0024
XREF	MSFT:MS10-024
XREF	OSVDB:64794
XREF	OSVDB:64793
XREF	OSVDB:63739
XREF	OSVDB:63738

Exploitable with

Core Impact (true)

Ports

tcp/445

```
- C:\WINNT\system32\inetsrv\Smtpsvc.dll has not been patched
    Remote version : 5.0.2195.6713
    Should be : 5.0.2195.7381
```

19405 - MS05-042: Vulnerability in Kerberos Could Allow Denial of Service, Information Disclosure and Spoofing (899587)

Description

The remote host contains a version of the Kerberos protocol that contains multiple security flaws that could allow an attacker to crash the remote service (AD), disclose information or spoof a session.
An attacker would need valid credentials to exploit these flaws.

Risk Factor

Medium

CVSS Base Score

4.6 (CVSS2#AV:N/AC:H/Au:S/C:P/I:P/A:P)

CVSS Temporal Score

3.4 (CVSS2#AV:N/AC:H/Au:S/C:P/I:P/A:P)

References

BID	14520
BID	14519
CVE	CVE-2005-1982
CVE	CVE-2005-1981
XREF	MSFT:MS05-042
XREF	OSVDB:18609
XREF	OSVDB:18608

Ports

tcp/445

```
- C:\WINNT\system32\kerberos.dll has not been patched
    Remote version : 5.0.2195.6666
    Should be : 5.0.2195.7053
```

19998 - MS05-045: Vulnerability in Network Connection Manager Could Allow Denial of Service (905414)

Description

The remote host contains a version of the Network Connection Manager that contains a denial of service vulnerability that could allow an attacker to disable the component responsible for managing network and remote access connections.
To exploit this vulnerability, an attacker would need to send a malformed packet to the remote host.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

CVE	CVE-2005-2307
XREF	MSFT:MS05-045
XREF	OSVDB:17885

Ports

tcp/445

```
- C:\WINNT\system32\netman.dll has not been patched
    Remote version : 5.0.2195.6660
    Should be : 5.0.2195.7061
```

23835 - MS06-076: Cumulative Security Update for Outlook Express (923694)

Description

The remote host is running a version of Microsoft Outlook Express that contains a security flaw that may allow an attacker to execute arbitrary code on the remote host.
To exploit this flaw, an attacker would need to send a malformed HTML email to a victim on the remote host and have him open it.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.0 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

References

BID	21501
CVE	CVE-2006-2386
XREF	MSFT:MS06-076
XREF	OSVDB:30821

Ports

tcp/445

```
- C:\WINNT\system32\Inetcomm.dll has not been patched
    Remote version : 5.50.4927.1200
    Should be : 5.50.4971.600
```

21693 - MS06-031: Vulnerability in RPC Mutual Authentication Could Allow Spoofing (917736)

Description

The remote version of Windows contains a version of SMB (Server Message Block) protocol that is vulnerable to a spoofing attack.
An attacker may exploit these flaws to enduce a user to connect to a malicious RPC server.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

References

BID	18389
CVE	CVE-2006-2380
XREF	MSFT:MS06-031
XREF	OSVDB:26438
XREF	CWE:287

Ports

tcp/445

```
- C:\WINNT\system32\Rpcrt4.dll has not been patched
    Remote version : 5.0.2195.6701
    Should be : 5.0.2195.7085
```

22028 - MS06-034: Vulnerability in Microsoft IIS using ASP Could Allow Remote Code Execution (917537)

Description

The remote host is running a version of Windows and IIS which is vulnerable to a flaw that could allow an attacker who has the privileges to upload arbitrary ASP scripts to it to execute arbitrary code.
Specifically, the remote version of IIS is vulnerable to a flaw when parsing specially crafted ASP files. By uploading a malicious ASP file on the remote host, an attacker may be able to take the complete control of the remote system.

Risk Factor

Medium

CVSS Base Score

6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)

CVSS Temporal Score

4.8 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)

References

BID	18858
CVE	CVE-2006-0026
XREF	MSFT:MS06-034
XREF	OSVDB:27152

Ports

tcp/445

```
- C:\WINNT\system32\inetsrv\asp.dll has not been patched
    Remote version : 5.0.2195.6672
    Should be : 5.0.2195.7084
```

45508 - MS10-021: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)

Description

The remote Windows host is running a version of the Windows kernel that is affected by eight vulnerabilities :

- A denial of service vulnerability exists in the Windows kernel due to the insufficient validation of registry keys passed to a Windows kernel system call. (CVE-2010-0234)
- A denial of service vulnerability exists in the Windows kernel due to the manner in which the kernel processes the values of symbolic links. (CVE-2010-0235)
- An elevation of privilege vulnerability exists in the Windows kernel due to the manner in which memory is allocated when extracting a symbolic link from a registry key. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. (CVE-2010-0236)
- An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. (CVE-2010-0237)
- A denial of service vulnerability exists in the way that the Windows kernel validates registry keys. (CVE-2010-0238)
- A denial of service vulnerability exists in the Windows kernel due to the way that the kernel resolves the real path for a registry key from its virtual path. (CVE-2010-0481)
- A denial of service vulnerability exists in the Windows kernel due to the improper validation of specially crafted image files. (CVE-2010-0482)
- A denial of service vulnerability exists in the Windows kernel due to the way that the kernel handles certain exceptions. (CVE-2010-0810)

Risk Factor

Medium

CVSS Base Score

6.2 (CVSS2#AV:L/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

4.9 (CVSS2#AV:L/AC:H/Au:N/C:C/I:C/A:C)

References

BID	39324
BID	39323
BID	39322
BID	39320
BID	39319
BID	39318
BID	39309
BID	39297
CVE	CVE-2010-0810
CVE	CVE-2010-0482
CVE	CVE-2010-0481
CVE	CVE-2010-0238
CVE	CVE-2010-0237
CVE	CVE-2010-0236
CVE	CVE-2010-0235
CVE	CVE-2010-0234
XREF	MSFT:MS10-021
XREF	IAVA:2010-A-0058

XREF	OSVDB:63736
XREF	OSVDB:63735
XREF	OSVDB:63733
XREF	OSVDB:63732
XREF	OSVDB:63731
XREF	OSVDB:63730
XREF	OSVDB:63729
XREF	OSVDB:63728

Ports
tcp/445

```
- C:\WINNT\system32\ntoskrnl.exe has not been patched
    Remote version : 5.0.2195.6717
    Should be : 5.0.2195.7376
```

16299 - MS03-034: NetBIOS Name Service Reply Information Leakage (824105) (credentialed check)

Description

The remote host is running a version of the NetBT name service that suffers from a memory disclosure problem.
An attacker could send a special packet to the remote NetBT name service, and the reply will contain random arbitrary data from the remote host memory. This arbitrary data may be a fragment from the web page the remote user is viewing, or something more serious like a POP password or anything else.
An attacker may use this flaw to continuously 'poll' the content of the memory of the remote host and might be able to obtain sensitive information.

Risk Factor

Low

CVSS Base Score

3.3 (CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.4 (CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N)

References

BID	8532
CVE	CVE-2003-0661
XREF	MSFT:MS03-034
XREF	OSVDB:2507

Ports
tcp/445

```
- C:\WINNT\system32\drivers\Netbt.sys has not been patched
    Remote version : 5.0.2195.6713
    Should be : 5.0.2195.6783
```

22333 - MS06-053: Vulnerability in Indexing Service Could Allow Cross-Site Scripting (920685)

Description

The remote host is running a version of the Indexing service that fails to adequately sanitize some requests.
Combined with a web server using this service, this flaw could be exploited by an attacker who would be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

2.1 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

References

BID	19927
CVE	CVE-2006-0032
XREF	MSFT:MS06-053
XREF	OSVDB:28729
XREF	CWE:79

Ports

tcp/445

```
- C:\WINNT\system32\Query.dll has not been patched
    Remote version : 5.0.2195.6664
    Should be : 5.0.2195.7100
```