Automated Scanning Vulnerability Report
Performed by Beyond Security's Automated Scanning
Host/s Tested: 192.168.4.122
Report Generated: 05 Jun 2007 13:31

Table of Contents	
Introduction	**Host Information**
Executive Summary	**Possible Vulnerabilities**
What Next?	

Introduction

We have scanned your host/s 192.168.4.122 for 4345 known security holes.

This scan took place on 5 Jun 2007 13:31 and took 0 hours and 5 minutes to complete.

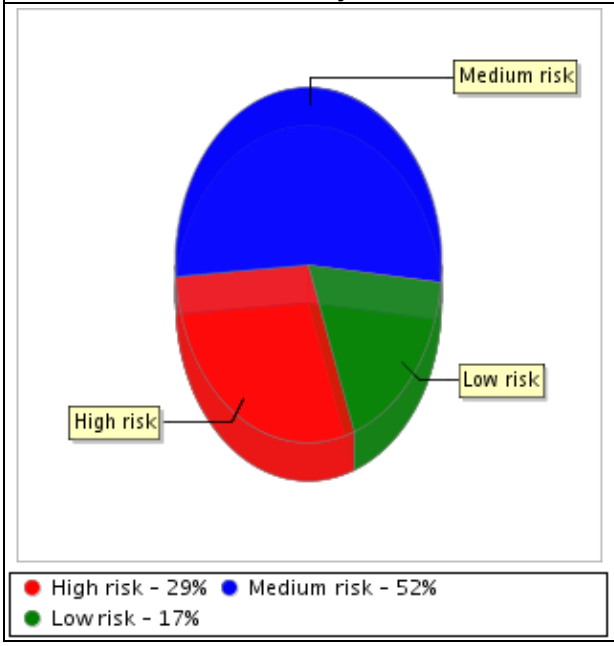
The '**Possible Vulnerabilities**' section of this report lists security holes found during the scan, sorted by risk level. Note that some of these reported vulnerabilities could be 'false alarms' since the hole is *never* actually exploited during the scan.

Some of what we found is purely informational; It will not help an attacker to gain access, but it will give him information about the local network or hosts. These results appear in the **'Low Risk / Intelligence Gathering'** section.

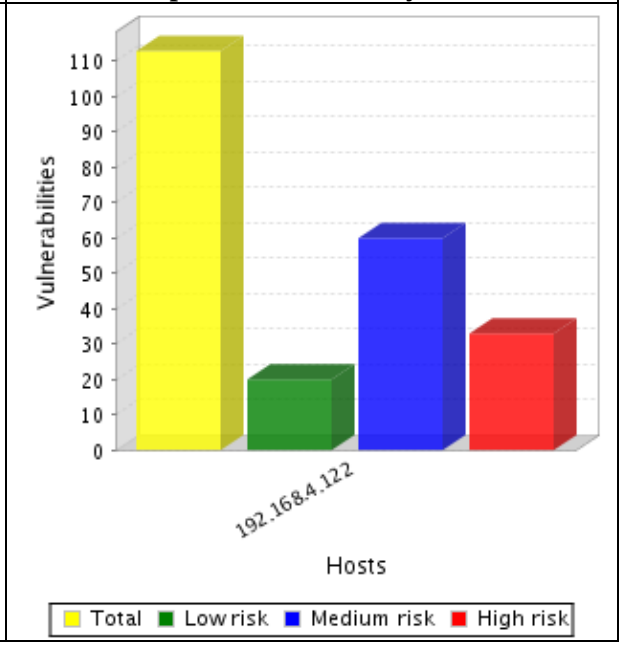
The last section of this report (**'Security Tests'**) lists the security tests that were performed in this scan by category of vulnerability.

Executive Summary				
Learn more about how vulnerabilities are classified				
Vulnerabilities by Host and Risk Level				
IP Address	**Total Vulnerabilities**	**High**	**Medium**	**Low**
192.168.4.122	113	33	60	20

Vulnerabilities By Risk Level

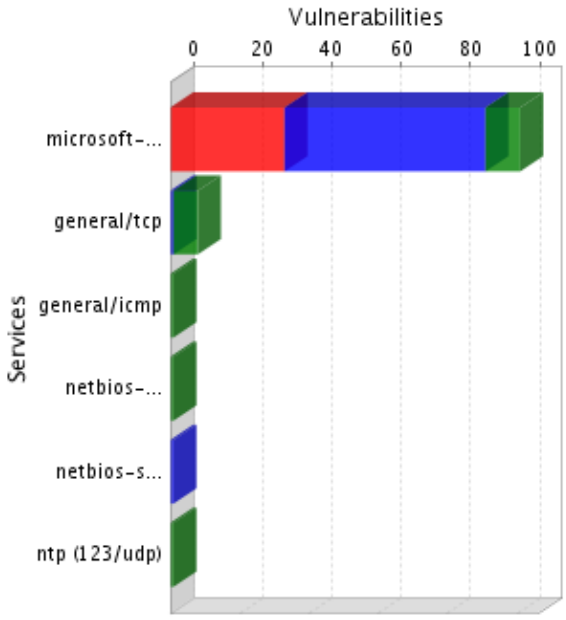


Top Vulnerabilities By Host

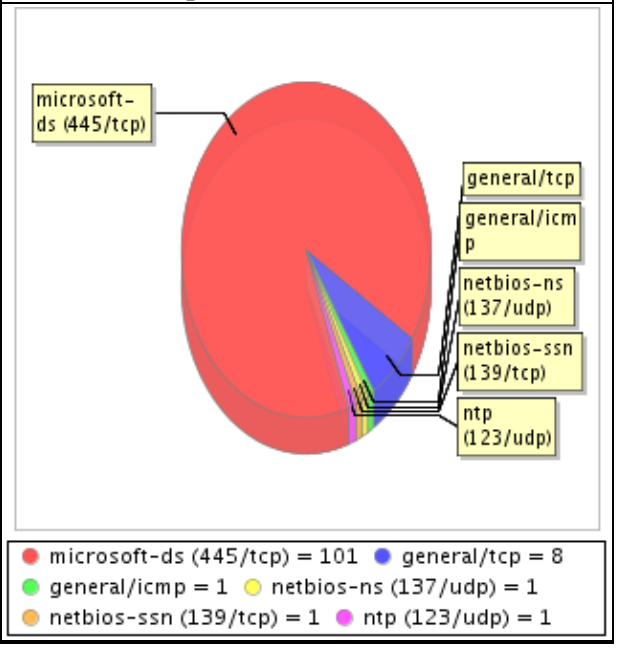


Vulnerabilities by Service and Risk Level				
Service	**Total Vulnerabilities**	**High Risk**	**Medium Risk**	**Low Risk**
netbios−ns (137/udp)	1	0	0	1
microsoft−ds (445/tcp)	101	33	58	10
general/tcp	8	0	1	7
ntp (123/udp)	1	0	0	1
netbios−ssn (139/tcp)	1	0	1	0
general/icmp	1	0	0	1

Top Vulnerabilities By Service



Top Vulnerable Services



Possible Vulnerabilities		
High	**Medium**	**Low**

Risk Factor: *High*
A Total of 33 *High Risk Vulnerability/ies was/were discovered.* (33 Uniq)

1. Vulnerability in Server Service Allows Code Execution (MS06−040, Network)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Buffer overflow in the Server Service in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allows remote attackers, including anonymous users, to execute arbitrary code via a crafted RPC message, a different vulnerability than CVE−2006−1314.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms06−040.mspx

CVE: CVE−2006−3439

TestID: 9923

2. Windows XP SP2 Firewall Critical Update (886185)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The remote version of Microsoft Windows XP SP2 lacks the critical security update 886185.

This update fixes a flaw which renders the Windows XP SP2's Firewall ineffective when the user connects to the Internet using a dialup connection.

Possible Solution: See solution provided at: http://support.microsoft.com/kb/886185

TestID: 6749

3. Vulnerability in DNS Resolution Allow Code Execution (MS06−041)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

There is a remote code execution vulnerability in Winsock that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system. For an attack to be successful the attacker would have to force the user to open a file or visit a website that is specially crafted to call the affected Winsock API. There is a remote code execution vulnerability in the DNS Client service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−041.mspx

CVE: CVE−2006−3440

TestID: 9894

4. Vulnerability in Microsoft JScript Allows Code Execution (MS06−023)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

There is a remote code execution vulnerability in JScript. An attacker could exploit the vulnerability by

constructing specially crafted JScript that could potentially allow remote code execution if a user visited a Web site or viewed a specially crafted e−mail message.

Impact: An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−023.mspx

CVE: CVE−2006−1313

TestID: 9789

5. Vulnerability in Plug and Play Allows Code Execution and Local Elevation of Privilege (MS05−047)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This update resolves a newly−discovered, privately−reported vulnerability. A remote code execution vulnerability exists in Plug and Play (PnP) that could allow an authenticated attacker who successfully exploited this vulnerability to take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. We recommend that customers apply the update at the earliest opportunity.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−047.mspx

CVE: CAN−2005−2120

TestID: 9289

6. Vulnerabilities in GDI Allows Code Execution (MS07−017)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Multiple vulnerabilities have been found in Microsoft's GDI:
* The Graphics Rendering Engine in Microsoft Windows 2000 SP4 and XP SP2 allows local users to gain privileges via "invalid application window sizes" in layered application windows, aka the "GDI Invalid Window Size Elevation of Privilege Vulnerability."

* The Graphics Rendering Engine in Microsoft Windows 2000 through 2000 SP4 and Windows XP through SP2 maps GDI Kernel structures on a global shared memory section that is mapped with read−only permissions, but can be remapped by other processes as read−write, which allows local users to cause a denial of service (memory corruption and crash) and gain privileges by modifying the kernel structures.

* Stack−based buffer overflow in the animated cursor code in Microsoft Windows 2000 SP4 through Vista allows remote attackers to execute arbitrary code or cause a denial of service (persistent reboot) via a large length value in the second (or later) anih block of a RIFF .ANI, cur, or .ico file, which results in memory corruption when processing cursors, animated cursors, and icons, a variant of CVE−2005−0416, as originally demonstrated using Internet Explorer 6 and 7.

* Unspecified kernel GDI functions in Microsoft Windows 2000 SP4; XP SP2; and Server 2003 Gold, SP1, and SP2 allows user−assisted remote attackers to cause a denial of service (possibly persistent restart) via a crafted Windows Metafile (WMF) image that causes an invalid dereference of an offset in a kernel structure, a related issue to CVE−2005−4560.

* Buffer overflow in the Graphics Device Interface (GDI) in Microsoft Windows 2000 SP4; XP SP2; Server 2003 Gold, SP1, and SP2; and Vista allows local users to gain privileges via a crafted Enhanced Metafile (EMF) image format file.

* The TrueType Fonts rasterizer in Microsoft Windows 2000 SP4 allows local users to gain privileges via crafted TrueType fonts, which result in an uninitialized function pointer.

* Buffer overflow in the Graphics Device Interface (GDI) in Microsoft Windows 2000 SP4; XP SP2; Server 2003 Gold, SP1, and SP2; and Vista allows local users to gain privileges via certain "color−related parameters" in crafted images.

* Unspecified vulnerability in Microsoft Windows 2000 SP4 through Vista allows remote attackers to execute arbitrary code or cause a denial of service (persistent reboot) via a malformed ANI file, which results in memory corruption when processing cursors, animated cursors, and icons, a similar issue to CVE−2005−0416, as originally demonstrated using Internet Explorer 6 and 7.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/Bulletin/MS07−017.mspx

CVE:
CVE−2006−5586,
CVE−2006−5758,
CVE−2007−0038,
CVE−2007−1211,
CVE−2007−1212,
CVE−2007−1213,
CVE−2007−1215,
CVE−2007−1765

TestID: 10327

7. Vulnerability in Windows Media Player Allows Code Execution (MS06−024)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A remote code execution vulnerability exists in Windows Media Player due to the way it handles the processing of PNG images. An attacker could exploit the vulnerability by constructing specially crafted Windows Media Player content that could potentially allow remote code execution if a user visits a malicious Web site or opens an email message with malicious content.

Impact: An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−024.mspx

CVE: CVE−2006−0025

TestID: 9788

8. Vulnerability in Server Message Block Allows Elevation of Privilege (MS06−030)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The Server Message Block (SMB) driver (MRXSMB.SYS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows local users to execute arbitrary code by calling the MrxSmbCscIoctlOpenForCopyChunk function with the METHOD_NEITHER method flag and an arbitrary address, possibly for kernel memory, aka the "SMB Driver Elevation of Privilege Vulnerability".

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−030.mspx

CVE: CVE−2006−2373

TestID: 9782

9. Vulnerability in Pragmatic General Multicast (PGM) Allow Code Execution (MS06−052)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

There is a remote code execution vulnerability that could allow an attacker to send a specially crafted multicast message to an affected system and execute code on the affected system. The MSMQ service, which is the Windows service needed to allow PGM communications is not installed by default.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−052.mspx

CVE: CVE−2006−3442

TestID: 9948

10. Vulnerability in Universal Plug and Play Allows Code Execution (MS07−019)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Stack−based buffer overflow in the Universal Plug and Play (UPnP) service in Microsoft Windows XP SP2 allows remote attackers on the same subnet to execute arbitrary code via crafted HTTP headers in request or notification messages, which trigger memory corruption.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms07−019.mspx

CVE: CVE−2007−1204

TestID: 10328

11. Vulnerability in Server Service Allows Code Execution (MS06−035, Network)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Heap−based buffer overflow in the Server Service (SRV.SYS driver) in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 up to SP1, and other products, allows remote attackers to execute arbitrary code via crafted first−class Mailslot messages that triggers memory corruption and bypasses size restrictions on second−class Mailslot messages. In addition, the Server Service (SRV.SYS driver) in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 up to SP1, and other products, allows remote attackers to obtain sensitive information via crafted requests that leak information in SMB buffers, which are not properly initialized, aka "SMB Information Disclosure Vulnerability."

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms06−035.mspx

CVE: CVE−2006−1314, CVE−2006−1315

TestID: 9875

12. Vulnerability in Telephony Service Allow Remote Code Execution (MS05−040)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A remote code execution vulnerability exists in Telephony Application Programming Interface (TAPI) that allows an attacker who successfully exploited this vulnerability to take complete control of the affected system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−040.mspx

CVE: CAN−2005−0058

TestID: 9121

13. Vulnerability in Windows Explorer Allows Code Execution (MS06−015)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A remote code execution vulnerability exists in Windows Explorer because of the way that it handles COM objects.

Impact: An attacker would need to convince a user to visit a Web site that could force a connection to a remote file server. This remote file server could then cause Windows Explorer to fail in a way that could allow code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Possible Solution: A solution can be found at:
http://www.microsoft.com/technet/security/bulletin/MS06−015.mspx

For More Information:
http://www.securiteam.com/windowsntfocus/5CP0J1PIAI.html

CVE: CVE−2006−0012

TestID: 9635

14. Cumulative Security Update for Internet Explorer (MS05−054)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

If a user is logged on with administrative user rights, an attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system.

Impact: An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−054.mspx

CVE: CAN−2005−1790

TestID: 9403

15. Vulnerability in Server Service Allows Code Execution (MS06−040)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

There is a remote code execution vulnerability in Server Service that could allow an attacker who success fully exploited this vulnerability to take complete control of the affected system.

Possible Solution: http://www.microsoft.com/technet/security/bulletin/MS06−040.mspx

CVE: CVE−2006−3439

TestID: 9867

16. Vulnerability in DHCP Client Service Could Allow Remote Code Execution (MS06−036)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

There is a remote code execution vulnerability in the DHCP Client service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−036.mspx

For More Information:
http://www.securiteam.com/windowsntfocus/5LP0J0KJ5E.html

CVE: CVE−2006−2372

TestID: 9843

17. Vulnerability in Vector Markup Language Allows Code Execution (MS06−055)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Stack−based buffer overflow in the Vector Graphics Rendering engine (vgx.dll), as used in Microsoft Outlook and Internet Explorer 6.0 on Windows XP SP2, and possibly other versions, allows remote attackers to execute arbitrary code via a Vector Markup Language (VML) file with a long fill parameter within a rect tag.

Possible Solution: A solution has been provided at:
http://www.microsoft.com/technet/security/Bulletin/MS06−055.mspx

CVE: CVE−2006−4868

TestID: 9996

18. Vulnerability in Graphics Rendering Engine Allow Remote Code Execution (MS06−001)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. We recommend that customers apply the update immediately

Possible Solution: http://www.microsoft.com/technet/security/bulletin/MS06−001.mspx

For More Information:
http://www.securiteam.com/windowsntfocus/5XP052AHFU.html

http://blogs.securiteam.com/index.php/archives/196

CVE: CVE−2005−4560

TestID: 9419

19. Vulnerability in Server Service Could Allow Remote Code Execution (MS06−035)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

There is a remote code execution vulnerability in the Server driver that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system. There is also an information disclosure vulnerability in the Server service that could allow an attacker to view fragments of memory used to store SMB traffic during transport.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−035.mspx

For More Information:
http://www.securiteam.com/windowsntfocus/5GP0E0KJ5G.html

CVE: CVE−2006−1314

TestID: 9842

20. Vulnerabilities in MSDTC and COM+ Allows Code Execution (MS05−051)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A remote code execution and local elevation of privilege vulnerability exists in the Microsoft Distributed Transaction Coordinator that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system. A remote code execution and local elevation of privilege vulnerability exists in COM+ that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

Impact: An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system.

An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. We recommend that Windows 2000 and Windows XP Service Pack 1 customers apply the update immediately.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−051.mspx

CVE: CAN−2005−1978

TestID: 9292

21. Vulnerabilities in Macromedia Flash Player from Adobe Allow Remote Code Execution (MS06−020)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This update resolves publicly reported vulnerabilities. These vulnerabilities are also documented in Macromedia Security Bulletin MPSB05−07 for customers using Flash Player 5 and 6. Customers who have installed Flash Player 7 and higher are advised to download the latest version from the Adobe website. Customers that have followed the guidance in Adobe Security Bulletin APSB06−03 are not at

risk from the vulnerability.

Impact: If a user is logged on with administrative user rights, an attacker who successfully exploited these vulnerabilities could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−020.mspx

For More Information:
http://www.securiteam.com/windowsntfocus/5XP0B00IKM.html or
http://www.adobe.com/devnet/security/security_zone/mpsb05−07.html

CVE: CVE−2006−0024

TestID: 9721

22. Vulnerability in Windows Could Allow Elevation of Privilege (MS06−075)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This update resolves a public vulnerability. We recommend that customers apply the update at the earliest opportunity.

Possible Solution: http://www.microsoft.com/technet/security/bulletin/MS06−075.mspx

TestID: 10107

23. Vulnerability in HTML Help Allows Remote Code Execution (MS05−026)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/Bulletin/MS05−026.mspx

CVE: CAN−2005−1208

TestID: 8943

24. Vulnerability in Print Spooler Service Allows Code Execution (MS05−043)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A vulnerability exists in the Print Spooler service that allows remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−043.mspx

CVE: CAN−2005−1984

TestID: 9123

25. Vulnerability in Microsoft Agent Allows Code Execution (MS06−068)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This update resolves a newly discovered, privately reported vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Impact: If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−068.mspx

CVE: CVE−2006−3445

TestID: 10052

26. Vulnerabilities in Windows Shell Allows Code Execution (MS05−049)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. However, user interaction is required to exploit this vulnerability. We recommend that customers apply the update at the earliest opportunity.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−049.mspx

CVE: CAN−2005−2122

TestID: 9290

27. Vulnerability in Microsoft Color Management Module Allows Code Execution (Registry, MS05−036)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A remote code execution vulnerability exists in the Microsoft Color Management Module because of the way that it handles ICC profile format tag validation. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Possible Solution: http://www.microsoft.com/technet/security/bulletin/MS05−036.mspx

For More Information:
For more information see: http://www.securiteam.com/windowsntfocus/5WP0B0UGAO.html

CVE: CAN−2005−1219

TestID: 9041

28. Vulnerability in Server Message Block Allows Remote Code Execution (MS05−027)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A remote code execution vulnerability exists in Server Message Block (SMB) that allows an attacker who successfully exploited this vulnerable to take complete control of the affected system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms05−027.mspx

CVE: CAN−2005−1208

TestID: 8944

29. Vulnerability in Plug and Play Allows Code Execution and Elevation of Privilege (MS05−039)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A remote code execution vulnerability exists in Plug and Play (PnP) allows an attacker who successfully exploited this vulnerability to take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−039.mspx

CVE: CAN−2005−1983

TestID: 9120

30. Vulnerability in Web Client Service Allows Code Execution (MS06−008, Network)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Buffer overflow in the Web Client service (WebClnt.dll) for Microsoft Windows XP SP1 and SP2, and Server 2003 up to SP1, allows remote authenticated users or Guests to execute arbitrary code via crafted RPC requests.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms06−008.mspx

CVE: CVE−2006−0013

TestID: 9558

31. Vulnerability in Windows Media Format Could Allow Remote Code Execution (MS06−078)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This update resolves a newly discovered, privately reported vulnerability. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

Possible Solution: http://www.microsoft.com/technet/security/bulletin/MS06−078.mspx

TestID: 10104

32. Vulnerabilities in CSRSS Allows Code Execution (MS07−021)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Multiple vulnerabilities have been discovered in Microsoft's CSRSS service:
* Double−free vulnerability in Microsoft Windows 2000, XP, 2003, and Vista allows local users to gain privileges by calling the MessageBox function with a MB_SERVICE_NOTIFICATION message with crafted data, which sends a HardError message to Client/Server Runtime Server Subsystem (CSRSS) process, which is not properly handled when invoking the UserHardError and GetHardErrorText functions in WINSRV.DLL.

* The Client Server Run−Time Subsystem (CSRSS) in Microsoft Windows allows local users to cause a denial of service (crash) or read arbitrary memory from csrss.exe via crafted arguments to the NtRaiseHardError function with status 0x50000018, a different vulnerability than CVE−2006−6696.

* Use−after−free vulnerability in the Client/Server Run−time Subsystem (CSRSS) in Microsoft Windows Vista does not properly handle connection resources when starting and stopping processes, which allows local users to gain privileges by opening and closing multiple ApiPort connections, which leaves a "dangling pointer" to a process data structure.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/Bulletin/MS07−021.mspx

CVE:
CVE−2006−6696,
CVE−2006−6797,
CVE−2007−1209

TestID: 10330

33. Vulnerability in SMB Allows Code Execution (MS05−027, Network Check)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that allows an attacker to execute arbitrary code on the remote host.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms05−027.mspx

CVE: CVE−2005−1206

TestID: 8978

Risk Factor: *Medium*
A Total of 59 *Medium Risk Vulnerability/ies was/were discovered.* (59 Uniq)

1. Flash Player Improper Memory Access Vulnerabilities
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

According to its version number, the instance of Macromedia's Flash Player on the remote host fails to validate the frame type identifier from SWF files before using that as an index into an array of function pointers. An attacker may be able to leverage this issue using a specially crafted SWF file to execute arbitrary code on the remote host subject to the permissions of the user running Flash Player.

Possible Solution: Upgrade to Flash Player version 7r61, version 8 or newer.

For More Information:
http://www.eeye.com/html/research/advisories/AD20051104.html,
http://www.sec−consult.com/228.html or
http://www.macromedia.com/devnet/security/security_zone/mpsb05−07.html

CVE: CVE−2005−2628, CVE−2005−3591

TestID: 9357

2. Vulnerability in JView Profiler Allows Code Execution (MS05−037)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The remote host contains a version of the JView Profiler module that is vulnerable to a security flaw which may 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.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms05−037.mspx

CVE: CVE−2005−2087

TestID: 9075

3. Vulnerability in Microsoft OLE Dialog Allows Code Execution (MS07−011)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The OLE Dialog component in Microsoft Windows 2000 SP4, XP SP2, and 2003 SP1 allows user−assisted remote attackers to execute arbitrary code via an RTF file with a malformed OLE object that triggers memory corruption.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/Bulletin/MS07−011.mspx

CVE: CVE−2007−0026

TestID: 10236

4. Vulnerability in TCP/IP Allow DoS (MS06−007)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A denial of service vulnerability exists that could allow an attacker to send a specially crafted IGMP packet to an affected system. An attacker could cause the affected system to stop responding.

Possible Solution: http://www.microsoft.com/technet/security/bulletin/MS06−007.mspx

CVE: CAN−2006−0021

TestID: 9509

5. Cumulative Security Update for Outlook Express (MS06−016)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A remote code execution vulnerability exists in Outlook Express when using a Windows Address Book (.wab) file that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

Impact: If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−016.mspx

For More Information:
http://www.securiteam.com/unixfocus/5YP0F1PIAW.html

CVE: CVE−2006−0014

TestID: 9636

6. Cumulative Security Update for Internet Explorer (MS06−021)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

If a user is logged on with administrative user rights, an attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. A remote code execution vulnerability exists in the way Internet Explorer handles exceptional conditions. As a result, system memory may be corrupted in such a way that an attacker could execute arbitrary code if a user visited a specially crafted Web site.

Impact: An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−021.mspx

CVE: CVE−2006−2218

TestID: 9791

7. Cumulative Security Update for Internet Explorer (MS07−016)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Microsoft Internet Explorer 5.01, 6, and 7 uses certain COM objects from Imjpcksid.dll as ActiveX controls, which allows remote attackers to execute arbitrary code via unspecified vectors. NOTE: this issue might be related to CVE−2006−4193.

In addition, Microsoft Internet Explorer 5.01, 6, and 7 uses certain COM objects from Msb1fren.dll, Htmlmm.ocx, and Blnmgrps.dll as ActiveX controls, which allows remote attackers to execute arbitrary code via unspecified vectors, a different issue than CVE−2006−4697.

In addition, the wininet.dll FTP client code in Microsoft Internet Explorer 5.01 and 6 might allow remote attackers to execute arbitrary code via an FTP server response of a specific length that causes a terminating null byte to be written outside of a buffer, which causes heap corruption.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/Bulletin/MS07−016.mspx

CVE: CVE−2006−4697, CVE−2007−0219, CVE−2007−0217

TestID: 10241

8. Vulnerability in the DHTML Editing Component ActiveX Control Allow Remote Code Execution (MS05−013)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A cross−domain vulnerability exists in the Microsoft Dynamic HTML (DHTML) Editing Component ActiveX control that could allow information disclosure or remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited that page.

Impact: An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−013.mspx

CVE: CAN−2004−1319

TestID: 7107

9. Vulnerability in Microsoft RichEdit Allows Code Execution (MS07−013)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The RichEdit component in Microsoft Windows 2000 SP4, XP SP2, and 2003 SP1; Office 2000 SP3, XP SP3, 2003 SP2, and Office 2004 for Mac; and Learning Essentials for Microsoft Office 1.0, 1.1, and 1.5 allows user−assisted remote attackers to execute arbitrary code via a malformed OLE object in an RTF file, which triggers memory corruption.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/Bulletin/MS07−013.mspx

CVE: CVE−2006−1311

TestID: 10238

10. Cumulative Security Update for Internet Explorer (Registry, 890923, MS05−020)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This is a cumulative update that includes the functionality of all the previously−released updates for Internet Explorer 5.01, Internet Explorer 5.5, and Internet Explorer 6.0. Additionally, it eliminates the following three newly−discovered vulnerabilities:

− DHTML Object Memory Corruption Vulnerability − CAN−2005−0553

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles certain DHTML objects. An attacker could exploit the vulnerability by constructing a malicious Web page. This malicious Web page could allow remote code execution if a user visited a malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

− URL Parsing Memory Corruption Vulnerability − CAN−2005−0554

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles certain URLs. An attacker could exploit the vulnerability by constructing a malicious Web page. This malicious Web page could potentially allow remote code execution if a user visited a malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

− Content Advisor Memory Corruption Vulnerability − CAN−2005−0555

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles Content Advisor files. An attacker could exploit the vulnerability by constructing a specially crafted Content Advisor file. This malicious Content Advisor file could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e−mail message and accepted the installation of the file. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

This test supercedes MS01−055, MS01−058, MS02−005, MS02−066, MS02−068, MS03−004, MS03−014, MS03−015, MS03−020, MS03−032, MS03−040, MS03−048, MS04−004, MS04−025, MS04−038, MS05−014 and others.

Impact: Attackers can execute code on the server.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms05−020.mspx

CVE: CVE−2004−0842, CVE−2004−0727, CVE−2004−0216, CVE−2004−0839, CVE−2004−0844, CVE−2004−0843, CVE−2004−0841, CVE−2004−0845

TestID: 1619

11. Vulnerability in HTML Help ActiveX Control Allows Code Execution (MS07−008)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The HTML Help ActiveX control (Hhctrl.ocx) in Microsoft Windows 2000 SP3, XP SP2 and Professional, 2003 SP1 allows remote attackers to execute arbitrary code via unspecified functions, related to uninitialized parameters.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms07−008.mspx

CVE: CVE−2007−0214

TestID: 10233

12. Cumulative Security Update for Internet Explorer (MS05−038)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The remote host contains a version of the Internet Explorer which is vulnerable to multiple security flaws (JPEG Rendering, Web Folder, COM Object) that allows 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.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms05−038.mspx

CVE: CVE−2005−1988,CVE−2005−1989,CVE−2005−1990

TestID: 9147

13. Vulnerability in the Korean Input Method Editor Allow Elevation of Privilege (MS06−009)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A privilege elevation vulnerability exists in the Windows and Office Korean Input Method Editor (IME). This vulnerability could allow a malicious user to take complete control of an affected system. For an attack to be successful an attacker must be able to interactively logon to the affected system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−009.mspx

CVE: CVE−2006−0008

TestID: 9511

14. Vulnerability in Telnet Client Allows Information Disclosure (MS05−033)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The TELNET protocol allows virtual network terminals to be connected to over the Internet. The initial description of the telnet protocol was given in RFC854 in May 1983. Since then there have been many extra features added including encryption.

Flaws in handling of the NEW−ENVIRON TELNET command in multiple telnet clients allows an attacker to gain sensitive information about the victim's system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−033.mspx

CVE: CAN−2005−1205

TestID: 8948

15. Vulnerabilities in Microsoft Windows Hyperlink Object Library Allows Code Execution (MS06−050)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This update resolves two newly discovered vulnerabilities. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. User interaction is required for an attacker to exploit these vulnerabilities. We recommend that customers apply the update at the earliest opportunity.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−050.mspx

CVE: CVE−2006−3086

TestID: 9901

16. Cumulative Security Update for Internet Explorer (MS05−025)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The remote host is missing the IE cumulative security update 883939. The remote version of IE is vulnerable to several flaws that allows an attacker to execute arbitrary code on the remote host.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms05−025.mspx

CVE: CVE−2005−1211, CVE−2002−0648

TestID: 8969

17. Shared Directory Access (Login)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

We tried to access the password protected shared directory using several login/password combinations.
− NULL sessions are enabled on the remote host
− Remote users are authenticated as 'Guest'

Impact: Attackers have read/write access to your shares, and can possibly login to the server remotely. This is one of SANS' top 20 security vulnerabilities: http://www.sans.org/top20/#w3

Possible Solution: 1. Disable 'File and Printer' sharing for any network interface that is visible from the Internet.

Or

2. Restrict anonymous enumeration. While this does not block unauthenticated connections in Windows XP and 2003 completely, it will prevent critical information disclosure:

Windows XP Home Edition (Note: This also works in Windows 2000 and XP Professional):
a. Set the Following Registry Key:
HKLM\\System\\CurrentControlSet\\Control\\LSA\\RestrictAnonymous=2

b. Reboot to make the changes take effect.

Windows XP Professional Edition and Windows Server 2003:
a. Go to Administrative Tools −−> Local Security Policy −−> Local Policies −−> Security Options.

Make sure the following two policies are enabled:
Network Access: Do not allow anonymous enumeration of SAM accounts: Enabled (Default)
Network Access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled

This can also be accomplished using the following registry keys:
HKLM\\System\\CurrentControlSet\\Control\\Lsa\\RestrictAnonymous=1
HKLM\\System\\CurrentControlSet\\Control\\Lsa\\RestrictAnonymousSAM=1
b. Reboot to make the changes take effect.

Windows 2000:
a. Go to −−> Administrative Tools −−> Local Security Settings −−> Local Policies −−> Security Options
b. Select "Additional restrictions of anonymous connections" in the Policy pane on the right
c. From the pull down menu labeled "Local policy setting", select: "No access without explicit anonymous permissions"

d. Click OK
e. The registry setting equivalent is:
HKLM\\System\\CurrentControlSet\\Control\\Lsa\\RestrictAnonymous=2
f. Reboot to make the changes take effect.

Windows NT 4.0 (Service Pack 3 or later):
Set the Following Registry Key:
HKLM\\System\\CurrentControlSet\\Control\\LSA\\RestrictAnonymous=1

3. To completely block access to the port, use a firewall or an IPSec policy.

References:
http://support.microsoft.com/support/kb/articles/Q143/4/74.asp (NT 4)
http://support.microsoft.com/support/kb/articles/Q289/6/55.ASP (Win 2k)
http://support.microsoft.com/support/kb/articles/Q132/6/79.ASP (general explanation)

For More Information:
http://www.securiteam.com/windowsntfocus/3E5PUR5QAY.html

CVE: CVE−1999−0504, CVE−1999−0506, CVE−2000−0222, CVE−1999−0505, CVE−2002−1117

TestID: 1162

18. Multiple Vulnerabilities in Windows Kernel Allows Elevation of Privilege and DoS (MS05−018, Registry)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Multiple vulnerabilities have been discovered in the Windows Kernel. The vulnerabilities are: a buffer overflow in the font processing component, a buffer overflow in the object management component and a privilege escalation vulnerability via CSRSS.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms05−018.mspx

CVE: CVE−2005−0551, CVE−2005−0550, CVE−2005−0060

TestID: 8533

19. Vulnerabilities in TCP/IP Allow Remote Code Execution and DoS (MS05−019, Registry)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Number of networking related vulnerabilities fixed by MS05−019 security update were reported by Microsoft. Those vulnerabilities are: IP Validation, ICMP Connection Reset, ICMP Path MTU, TCP Connection Reset and Spoofed Connection Request.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms05−019.mspx

For More Information:
http://www.securiteam.com/exploits/5SP0C20FFY.html

CVE: CVE−2005−0048, CVE−2004−0790, CVE−2004−1060, CVE−2004−0230, CVE−2005−0688

TestID: 8534

20. Vulnerability in Remote Desktop Protocol DoS (MS05−041)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A denial of service vulnerability exists that could allow an attacker to send a specially crafted Remote Data Protocol (RDP) message to an affected system. An attacker could cause this system to stop responding.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−041.mspx

CVE: CAN−2005−1218

TestID: 9118

21. Vulnerabilities in TCP/IP IPv6 Allows DoS (MS06−064)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A denial of service vulnerability exists in Windows in the IPv6 implementation of TCP/IP.

Impact: An attacker who successfully exploited this vulnerability could cause the affected system to stop responding.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−064.mspx

CVE: CVE−2004−0230

TestID: 10015

22. Remotely Accessible Registry
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

We were able to access the registry remotely using the supplied credentials.

Impact: This allows attackers to read information from the registry, and possibly modify it.

Possible Solution: Restrict outside access to the NetBIOS port.

For More Information:
http://www.securiteam.com/windowsntfocus/3E5PUR5QAY.html

CVE: CVE−1999−0562

TestID: 1164

23. Vulnerability in Microsoft Agent Allows Code Execution (MS07−020)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Unspecified vulnerability in Microsoft Agent (msagent\agentsvr.exe) in Windows 2000 SP4, XP SP2, and Server 2003, 2003 SP1, and 2003 SP2 allows remote attackers to execute arbitrary code via crafted URLs, which result in memory corruption.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms07−020.mspx

CVE: CVE−2007−1205

TestID: 10329

24. Vulnerability in Microsoft Distributed Transaction Coordinator Allows DoS (MS06−018)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A denial of service vulnerability exists that could allow an attacker to send a specially crafted network message to an affected system. An attacker could cause the Microsoft Distributed Transaction Coordinator (MSDTC) to stop responding. Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but it could cause the affected system to stop accepting requests.

Impact: An attacker could cause the Microsoft Distributed Transaction Coordinator (MSDTC) to stop responding. Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but it could cause the affected system to stop accepting requests.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−018.mspx

For More Information:
http://www.securiteam.com/windowsntfocus/5YP0C00IKI.html

CVE: CVE−2006−0034

TestID: 9716

25. Vulnerability in Microsoft Data Access Components Allows Code Execution (MS07−009)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The Execute method in the ADODB.Connection 2.7 and 2.8 ActiveX control objects (ADODB.Connection.2.7 and ADODB.Connection.2.8) does not properly track freed memory when the second argument is a BSTR, which allows remote attackers to cause a denial of service (Internet Explorer crash) and possibly execute arbitrary code via certain strings in the second and third arguments.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms07−009.mspx

CVE: CVE−2006−5559

TestID: 10234

26. Cumulative Security Update for Outlook Express (MS06−076)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Unspecified vulnerability in Microsoft Outlook Express 6 and earlier allows remote attackers to execute arbitrary code via a crafted contact record in a Windows Address Book (WAB) file.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms06−076.mspx

CVE: CVE−2006−2386

TestID: 10132

27. Flash Player APSB06−03
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Multiple unspecified vulnerabilities in Adobe Flash Player 8.0.22.0 and earlier allow remote attackers to execute arbitrary code via a crafted SWF file.

Possible Solution: Upgrade to Flash Player version 7.0.63.0, version 8.0.24.0 or newer.

For More Information:
http://www.microsoft.com/technet/security/advisory/916208.mspx and
http://www.macromedia.com/devnet/security/security_zone/apsb06−03.html

CVE: CVE−2006−0024

TestID: 9615

28. Vulnerability in Windows Image Acquisition Service Allows Elevation of Privilege (MS07−007)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The Window Image Acquisition (WIA) Service in Microsoft Windows XP SP2 allows local users to gain privileges via unspecified vectors involving an "unchecked buffer," probably a buffer overflow.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms07−007.mspx

CVE: CVE−2007−0210

TestID: 10232

29. Vulnerabilities in Kerberos Allows DoS, Information Disclosure, and Spoofing (MS05−042)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This is an information disclosure and spoofing vulnerability. This vulnerability allows an attacker to tamper with certain information that is sent from a domain controller and potentially access sensitive client network communication. Users could believe they are accessing a trusted server when in reality they are accessing a malicious server. However, an attacker would first have to inject themselves into the middle of an authentication session between a client and a domain controller. Also, a denial of service vulnerability exists that could allow an attacker to send a specially crafted message to a Windows domain controller that could cause the service that is responsible for authenticating users in an Active Directory domain to stop responding.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−042.mspx

CVE: CAN−2005−1981,CAN−2005−1981

TestID: 9122

30. Vulnerability in the Client Service for NetWare Allows Code Execution (MS05−046)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This update resolves a newly−discovered, privately−reported vulnerability. A remote code execution vulnerability exists in the Client Service for NetWare (CSNW). By default, CSNW is not installed on any affected operating system version. Only customers who manually installed CSNW could be vulnerable to this issue. This service is also called Gateway Service for NetWare on Windows 2000 Server.

Impact: An attacker who successfully exploited this vulnerability could remotely take complete control of an affected system.

An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. We recommend that customers apply the update at the earliest opportunity.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−046.mspx

CVE: CAN−2005−1985

TestID: 9288

31. Vulnerability in Windows Shell Allows Elevation of Privilege (MS07−006)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The hardware detection functionality in the Windows Shell in Microsoft Windows XP SP2 and Professional, and Server 2003 SP1 allows local users to gain privileges via an unvalidated parameter to a function related to the "detection and registration of new hardware."

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms07−006.mspx

CVE: CVE−2007−0211

TestID: 10231

32. Vulnerability in Microsoft Agent Allows Spoofing (MS05−032)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This is a spoofing vulnerability that exists in the affected products and that could enable an attacker to spoof trusted Internet content. Users could believe that they are accessing trusted Internet content.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/Bulletin/MS05−032.mspx

CVE: CAN−2005−1214

TestID: 8947

33. SMB Shares Enumeration
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The following shares are accessible from the outside (without requiring a valid username or password):

IPC$
SharedDocs
beSTORM project
ADMIN$
C$

Impact: Attackers can access those shares remotely.

Possible Solution: Restrict access to those shares by a password, and filter the NetBIOS port from

outside access.

For More Information:
http://www.securiteam.com/windowsntfocus/3E5PUR5QAY.html

TestID: 1151

34. Flash Player Running Version Prior to 9.0
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Unspecified vulnerability in Macromedia Flash Player 8.0.24.0 allows remote attackers to execute arbitrary commands via a malformed .swf file that results in "multiple improper memory access" errors. In addition, an unspecified vulnerability in Macromedia Flash Player 8.0.24.0 allows remote attackers to cause a denial of service (browser crash) via a malformed, compressed .swf file.

Possible Solution: Upgrade to Flash Player version 9.0 or newer.

For More Information:
http://www.fortinet.com/FortiGuardCenter/advisory/FG−2006−20.html,
http://www.fortinet.com/FortiGuardCenter/advisory/FG−2006−21.html, or
http://www.kb.cert.org/vuls/id/474593

CVE: CVE−2006−3587, CVE−2006−3588

TestID: 9869

35. Vulnerability in Hyperlink Object Library Allows Code Execution (MS05−015)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A remote code execution vulnerability exists in the Hyperlink Object Library. This problem exists because of an unchecked buffer while handling hyperlinks. An attacker could exploit the vulnerability by constructing a malicious hyperlink which could potentially lead to remote code execution if a user clicks a malicious link within a Web site or e−mail message.

Impact: An attacker who successfully exploited this vulnerability could take complete control of the affected system. User interaction is required to exploit this vulnerability.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−015.mspx

CVE: CAN−2005−0057

TestID: 7108

36. Vulnerability in Web Client Service Allow Remote Code Execution (MS06−008)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. We recommend that customers apply the update at the earliest opportunity.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−008.mspx

CVE: CVE−2006−0013

TestID: 9510

37. Vulnerability in HTML Help Allows Code Execution (MS06−046)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A vulnerability exists in the HTML Help ActiveX control that could allow remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited that page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−046.mspx

CVE: CVE−2006−3357

TestID: 9899

38. Vulnerability in Microsoft Windows Code Execution (MS06−043)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

There is a remote code execution vulnerability in Windows that results from incorrect parsing of the MHTML protocol. An attacker could exploit the vulnerability by constructing a specially crafted Web page or HTML e−mail that could potentially lead to remote code execution if a user visited a specially crafted Web site or clicked a link in a specially crafted e−mail message. If a user were logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system.

Impact: An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−043.mspx

CVE: CVE−2006−2766

TestID: 9896

39. Cumulative Security Update for Internet Explorer (MS06−067)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Heap−based buffer overflow in DirectAnimation.PathControl COM object (daxctle.ocx) in Microsoft Internet Explorer 6.0 SP1 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a Spline function call whose first argument specifies a large number of points.

In addition, a heap−based buffer overflow in the DirectAnimation Path Control (DirectAnimation.PathControl) COM object (daxctle.ocx) for Internet Explorer 6.0 SP1, on Chinese and possibly other Windows distributions, allows remote attackers to execute arbitrary code via unknown manipulations in arguments to the KeyFrame method, possibly related to an integer overflow, as demonstrated by daxctle2, and a different vulnerability than CVE−2006−4446.

Finally, Microsoft Internet Explorer 5.01 through 6 allows remote attackers to execute arbitrary code via crafted layout combinations involving DIV tags and HTML CSS float properties that trigger memory corruption, aka "HTML Rendering Memory Corruption Vulnerability."

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/Bulletin/MS06−067.mspx

CVE: CVE−2006−4446, CVE−2006−4777, CVE−2006−4687

TestID: 10071

40. Vulnerability in DirectShow Allows Code Execution (MS05−050)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. We recommend that customers apply the update immediately.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−050.mspx

CVE: CAN−2005−2128

TestID: 9291

41. Cumulative Security Update for Internet Explorer (MS05−052, 896688)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The remote host contains a version of the Internet Explorer which is vulnerable to a security flaw (COM Object Instantiation Memory Corruption Vulnerability) that allows 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.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms05−052.mspx

CVE: CVE−2005−2127

TestID: 9327

42. Vulnerability in Microsoft MFC Allows Code Execution (MS07−012)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The MFC component in Microsoft Windows 2000 SP4, XP SP2, and 2003 SP1 and Visual Studio .NET 2000, 2000 SP1, 2003, and 2003 SP1 allows user−assisted remote attackers to execute arbitrary code via an RTF file with a malformed OLE object that triggers memory corruption.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/Bulletin/MS07−012.mspx

CVE: CVE−2007−0025

TestID: 10237

43. Vulnerability in Network Connection Manager Allow DoS (MS05−045)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This update resolves a newly−discovered, public vulnerability. A vulnerability in Network Connection Manager could allow a denial of service on the affected platforms against the Network Connection

Manager. An attacker who successfully exploited this vulnerability could cause the component responsible for managing network and remote access connections to stop responding. If the affected component is stopped due to an attack, it will automatically restart when new requests are received. We recommend that customers consider applying the security update.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−045.mspx

CVE: CAN−2005−2307

TestID: 9287

44. Vulnerability in Windows Kernel Allows Elevation of Privilege (MS07−022)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The Virtual DOS Machine (VDM) in the Windows Kernel in Microsoft Windows NT 4.0; 2000 SP4; XP SP2; Server 2003, 2003 SP1, and 2003 SP2; and Windows Vista before June 2006; uses insecure permissions (PAGE_READWRITE) for a physical memory view, which allows local users to gain privileges by modifying the "zero page" during a race condition before the view is unmapped.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms07−022.mspx

CVE: CVE−2007−1206

TestID: 10331

45. Users in the 'Admin' Group
Hosts affected: 192.168.4.122 (port: general/tcp)

Using the supplied credentials it was possible to extract the member list of group 'Administrators'. Members of this group have a complete access to the remote system.

You should make sure that only the proper users are member of this group.

. Administrator (User)
. Support (User)

Impact: This information might be sensitive and should not be revealed.

Possible Solution: You should make sure that only the proper users are member of this group.

TestID: 1655

46. Vulnerability in Windows Explorer Allows Code Execution (MS06−045)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Microsoft Internet Explorer 6.0 does not properly handle Drag and Drop events, which allows remote user−complicit attackers to execute arbitrary code via a link to an SMB file share with a filename that contains encoded ..\ (%2e%2e%5c) sequences and whose extension contains the CLSID Key identifier for HTML Applications (HTA), aka "Folder GUID Code Execution Vulnerability." NOTE: directory traversal sequences were used in the original exploit, although their role is not clear.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/Bulletin/MS06−045.mspx

CVE: CVE−2006−3281

TestID: 9898

47. Vulnerability in Vector Markup Language Allows Code Execution (MS07−004)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Integer overflow in the Vector Markup Language (VML) implementation (vgx.dll) in Microsoft Internet Explorer 5.01, 6, and 7 on Windows 2000 SP4, XP SP2, Server 2003, and Server 2003 SP1 allows remote attackers to execute arbitrary code via a crafted web page that contains unspecified integer properties that cause insufficient memory allocation and trigger a buffer overflow, aka the "VML Buffer Overrun Vulnerability."

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/Bulletin/MS07−004.mspx

CVE: CVE−2007−0024

TestID: 10184

48. Vulnerabilities in Graphics Rendering Engine Allows Code Exection (MS05−053)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The remote host contains a version of Microsoft Windows is missing a critical security update which fixes several vulnerabilities in the Graphic Rendering Engine, and in the way Windows handles Metafiles.

Impact: An attacker may exploit these flaws to execute arbitrary code on the remote host. To exploit these flaws, an attacker would need to send 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 allows the execution of arbitrary code with the privileges of the user.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms05−053.mspx

CVE: CVE−2005−2123, CVE−2005−2124, CVE−2005−0803

TestID: 9356

49. Vulnerability in the Client Service for NetWare Allows Code Execution (MS06−066)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Buffer overflow in Client Service for NetWare (CSNW) in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 up to SP1 allows remote attackers to execute arbitrary code via crafted messages, aka "Client Service for NetWare Memory Corruption Vulnerability."

In addition, an unspecified vulnerability in the driver for the Client Service for NetWare (CSNW) in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 up to SP1 allows remote attackers to cause a denial of service (hang and reboot) via has unknown attack vectors, aka "NetWare Driver Denial of Service Vulnerability."

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms06−066.mspx

CVE: CVE−2006−4688, CVE−2006−4689

TestID: 10070

50. Vulnerability in Windows Shell Allows Code Execution (MS05−016, Registry)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

A remote code execution vulnerability exists in the Windows Shell because of the way that it handles application association. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of the affected system. However, user interaction is required to exploit this vulnerability.

To exploit this flaw, an attacker would need to lure a victim into visiting a malicious website or into opening a malicious file attachment.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS05−016.mspx

CVE: CVE−2005−0063

TestID: 8531

51. SMB Listens on Port
No of hosts affected: 2
Hosts affected: 192.168.4.122 (port: netbios−ssn (139/tcp)), 192.168.4.122 (port: microsoft−ds (445/tcp))

Ports 139 and 445 are used for 'NetBIOS' communication between two Windows 2000 hosts. In the case of port 445 an attacker may use this to perform NetBIOS attacks as it would on port 139.

Impact: All NetBIOS attacks are possible on this host.

Possible Solution: Filter incoming traffic to this port.

TestID: 1782

52. Vulnerability in Windows Media Player Plug−in Allows Code Execution (MS06−006)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Buffer overflow in the plug−in for Microsoft Windows Media Player (WMP) 9 and 10, when used in browsers other than Internet Explorer and set as the default application to handle media files, allows remote attackers to execute arbitrary code via HTML with an EMBED element containing a long src attribute.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms06−006.mspx

CVE: CVE−2006−0005

TestID: 9560

53. Vulnerability in Windows Explorer Allows Remote Execution (MS06−057)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Integer overflow in Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) and execute arbitrary code via a 0x7fffffff argument to the setSlice method on a WebViewFolderIcon ActiveX object, which leads to an invalid memory copy. This causes an invalid memory copy and may result in arbitrary code execution and/or a loss of availability for the browser.

Impact: An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−057.mspx

CVE: CVE−2006−3730

TestID: 10008

54. Vulnerability in PNG Processing Allows Code Execution (MS05−009)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The remote host is running either Windows Media Player 9 or MSN Messenger.

There is a vulnerability in the remote version of this Windows Media Player 9 or MSN Messenger allows an attacker to execute arbitrary code on the remote host. To exploit this flaw, one attacker would need to set up a rogue PNG image and send it to a victim on the remote host.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms05−009.mspx

CVE: CVE−2004−1244, CVE−2004−0597

TestID: 7187

55. Shared Directory Access (Share Access)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The remote has one or many Windows shares that can be accessed through the Network with the given credentials. Depending on the share rights, it may allow an attacker to read/write confidential data.

The following shares can be accessed as administrator:

− C$ − (readable,writable)
+ Content of this share :
boot.ini
CONFIG.SYS
Documents and Settings
IO.SYS
MSDOS.SYS
NTDETECT.COM
ntldr
pagefile.sys
Program Files
RECYCLER
System Volume Information
Temp
WINDOWS

− ADMIN$ − (readable,writable)
+ Content of this share :
..
0.log

addins
AppPatch
Blue Lace 16.bmp
bootstat.dat
clock.avi
cmsetacl.log
Coffee Bean.bmp
comsetup.log
Config
Connection Wizard
control.ini
Cursors
Debug
desktop.ini
Downloaded Program Files
Driver Cache
DtcInstall.log
ehome
explorer.exe
explorer.scf
FaxSetup.log
FeatherTexture.bmp
Fonts
Gone Fishing.bmp
Greenstone.bmp
Help
hh.exe
iis6.log
ime
imsins.log
inf
Installer
java
MedCtrOC.log
Media
msagent
msapps
msdfmap.ini
msgsocm.log
msmqinst.log
mui
netfxocm.log
NOTEPAD.EXE
nsw.log
ntdtcsetup.log
ocgen.log
ocmsn.log
ODBCINST.INI
OEWABLog.txt
Offline Web Pages
pchealth

PeerNet
Prairie Wind.bmp
Prefetch
Provisioning
regedit.exe
Registration
REGLOCS.OLD
regopt.log
repair
Resources
Rhododendron.bmp
River Sumida.bmp
Santa Fe Stucco.bmp
SchedLgU.Txt
security
sessmgr.setup.log
SET3.tmp
SET4.tmp
SET8.tmp
setupact.log
setupapi.log
setuperr.log
setuplog.txt
Soap Bubbles.bmp
SoftwareDistribution
srchasst
Sti_Trace.log
system
system.ini
system32
tabletoc.log
TASKMAN.EXE
Tasks
Temp
tsoc.log
twain.dll

− beSTORM project − (readable,writable)
+ Content of this share :
..
Copy of settings.bsp
exception1.txt
Logs
settings 2.bsp
settings.bsp

− SharedDocs − (readable,writable)
+ Content of this share :
..
desktop.ini
My Music

My Pictures
My Videos

Impact: Attackers can gain critical information about the host.

Possible Solution: Restrict access to those shares by a password, and filter the NetBIOS port from outside access.

For More Information:
http://www.securiteam.com/windowsntfocus/3E5PUR5QAY.html

CVE: CVE−1999−0519, CVE−1999−0520

TestID: 1170

56. SMB Host SID User Enumeration
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The host SID could be used to enumerate the names of the local users of this host (we only enumerated users name whose ID is between 1000 and 1200 for performance reasons). The following list can give additional knowledge to an attacker:
− Administrator account name : Administrator (id 500)
− Guest account name : Guest (id 501)
− HelpAssistant (id 1000)
− HelpServicesGroup (id 1001)
− SUPPORT_388945a0 (id 1002)
− Support (id 1003)

Impact: Attackers can gain critical information about the host.

Possible Solution: Restrict outside access to the NetBIOS port.

CVE: CVE−2000−1200

TestID: 1620

57. Vulnerability in Windows Kernel Could Result in Code Execution (MS06−051)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This update resolves newly discovered, privately reported vulnerabilities and additional issues discovered through internal investigations. An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. We recommend that customers apply the update immediately.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−051.mspx

CVE: CVE−2006−3648

TestID: 9904

58. Vulnerability in HTML Help Allows Code Execution (MS05−001, Registry Check)

Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This update resolves a newly−discovered, publicly reported vulnerability.

A vulnerability exists in the HTML Help ActiveX control in Windows that could allow information disclosure or remote code execution on an affected system. This vulnerability is documented in the Vulnerability Details section of this bulletin. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

Users whose accounts are configured to have fewer privileges on the system could be less impacted than users who operate with administrative privileges.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/ms05−001.mspx

CVE: CVE−2004−1043

TestID: 6882

59. Vulnerability in Routing and Remote Access Allows Code Execution (MS06−025)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Buffer overflow in the Routing and Remote Access service (RRAS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows remote unauthenticated or authenticated attackers to execute arbitrary code via certain crafted "RPC related requests," aka the "RRAS Memory Corruption Vulnerability."

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−025.mspx

CVE: CVE−2006−2370

TestID: 9787

Risk Factor: *Low*

A Total of 20 *Low Risk Vulnerability/ies was/were discovered.* (20 Uniq)

1. Local Users Information: Password Never Changed
Hosts affected: 192.168.4.122 (port: general/tcp)

Using the supplied credentials it was possible to extract the list of users who never changed their password. It is recommanded to allow/force users to change their password for security reasons.

HelpAssistant
SUPPORT_388945a0

Impact: Attackers can know which users still use the default password.

Possible Solution: You encourage let your users to periodically change their passwords.

TestID: 1674

2. Vulnerability in TCP/IP Allow Code Execution (MS06−032)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Buffer overflow in the TCP/IP Protocol driver in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows remote attackers to execute arbitrary code via unknown vectors related to IP source routing.

Possible Solution: See solution provided at:
http://www.microsoft.com/technet/security/bulletin/MS06−032.mspx

CVE: CVE−2006−2379

TestID: 9780

3. LANMAN Browse Listing
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This test tries to obtain the host browse list by connecting to: \\PIPE\\LANMAN. Here is the browse list of the remote host:

SECURITY−5FF191 (os: 5.1)
SUP1 (os: 4.9)

Impact: This gives the attacker information about other potential targets on the local network.

Possible Solution: Filter incoming communication to port 139.

TestID: 1150

4. SMB Services Enumeration
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This test implements tries to obtain, using the SMB protocol, the list of active services of the remote host. The results are:
Application Layer Gateway Service [ALG]
Windows Audio [AudioSrv]
Computer Browser [Browser]
Cryptographic Services [CryptSvc]
DCOM Server Process Launcher [DcomLaunch]
DHCP Client [Dhcp]
Logical Disk Manager [dmserver]
DNS Client [Dnscache]
Error Reporting Service [ERSvc]
Event Log [Eventlog]
COM+ Event System [EventSystem]
Fast User Switching Compatibility [FastUserSwitchingCompatibility]
Help and Support [helpsvc]
Server [lanmanserver]
Workstation [lanmanworkstation]
TCP/IP NetBIOS Helper [LmHosts]
Network Connections [Netman]
Network Location Awareness (NLA) [Nla]
Plug and Play [PlugPlay]
IPSEC Services [PolicyAgent]

Protected Storage [ProtectedStorage]
Remote Registry [RemoteRegistry]
Remote Procedure Call (RPC) [RpcSs]
Security Accounts Manager [SamSs]
Task Scheduler [Schedule]
Secondary Logon [seclogon]
System Event Notification [SENS]
Windows Firewall/Internet Connection Sharing (ICS) [SharedAccess]
Shell Hardware Detection [ShellHWDetection]
Print Spooler [Spooler]
System Restore Service [srservice]
SSDP Discovery Service [SSDPSRV]
Terminal Services [TermService]
Themes [Themes]
Distributed Link Tracking Client [TrkWks]
VMware Tools Service [VMTools]
Windows Time [W32Time]
WebClient [WebClient]
Windows Management Instrumentation [winmgmt]
Security Center [wscsvc]
Automatic Updates [wuauserv]
Wireless Zero Configuration [WZCSVC]

Impact: Attackers can gain critical information about the host.

Possible Solution: Block the NetBIOS ports from outside access.

For More Information:
http://www.securiteam.com/windowsntfocus/3E5PUR5QAY.html

TestID: 1179

5. Password Policy Retrieval
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

Using the supplied credentials it was possible to extract the password policy. Password policy must be conform to the Informationnal System Policy.

The following password policy is defined on the remote host:

Minimum password len: 0
Password history len: 0
Maximum password age (d): 42
Password must meet complexity requirements: Enabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

TestID: 8447

6. Local Users Information: Users Which Never Logged On
Hosts affected: 192.168.4.122 (port: general/tcp)

Using the supplied credentials it was possible to extract the list of local users who never logged into the remote host. It is recommanded to delete useless accounts.

Impact: Unused accounts make likely candidates for attack.

Possible Solution: You should delete unused accounts.

TestID: 1675

7. Host SID Information Retrieval
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

We obtained the domain (or host) Security Identifier (SID). The domain/host SID can be used to get the list of users of the domain or the list of local users.

The remote host SID value is:
1−5−21−1004336348−1708537768−725345543

Impact: Attackers can gain critical information about the host.

Possible Solution: Restrict outside access to the NetBIOS port.

CVE: CVE−2000−1200

TestID: 1618

8. Software License Compliance Check (BSA)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The following software is installed:

Windows XP − 5.1.2600

TestID: 6679

9. SMB Share Hosting Office Files
Hosts affected: 192.168.4.122 (port: general/tcp)

This test connects to the remotely accessible SMB shares and attempts to find office related files (such as .doc, .ppt, .xls, .pdf etc), if no authentication credentials have been provided this test has been able to gain access to sensitive files.

Here is a list of office files which have been found on the remote SMB shares:
+ beSTORM project :

exception1.txt

Possible Solution: Make sure that the files containing confidential information have proper access controls set on them.

TestID: 10168

10. Windows Messenger Detection
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The remote host is using Windows Messenger − an instant messenging software, which may not be suitable for a business environment.

Possible Solution: Remove/Disable the software if it is not required.

CVE: CVE−1999−1484, CVE−2002−0228, CVE−2002−0472

TestID: 2478

11. Winlogon Passwords Caching
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The registry key HKLM\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\CachedLogonsCount is non−null. It means that the remote host locally caches the passwords of the users when they log in, in order to continue to allow the users to log in in the case of the failure of the PDC.

Possible Solution: Use a registry editor to set the value of this key to 0.

TestID: 2408

12. NTP Variables Reading
Hosts affected: 192.168.4.122 (port: ntp (123/udp))

It is possible to determine a lot of information about the remote host by querying the NTP variables − these include OS descriptor, and time settings.

Theoretically one could work out the NTP peer relationships and track back network settings from this.

Impact: Attackers can gain critical information about the host.

Possible Solution: Set NTP to restrict default access to ignore all info packets: restrict default ignore

TestID: 1653

13. Windows XP Classic Logon Screen
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

The registry key HKLM\Software\Microsoft\Windows NT\WinLogon\LogonType does not exist or is set to 1.

It means that users who attempt to log in locally will see get the 'new' WindowsXP logon screen which displays the list of users of the remote host.

Possible Solution: Use a registry editor to set the value of this key to 0.

TestID: 2410

14. Local Users Information: Disabled Accounts
Hosts affected: 192.168.4.122 (port: general/tcp)

Using the supplied credentials it was possible to extract the disabled user account list. Permanently disabled accounts should be suppressed.

HelpAssistant

SUPPORT_388945a0

TestID: 1673

15. ICMP Timestamp Request
Hosts affected: 192.168.4.122 (port: general/icmp)

The remote host answers to an ICMP timestamp request. This allows an attacker to know the time and date on your host.

Impact: This may help attackers to defeat time based authentications schemes.

Possible Solution: Filter out the ICMP timestamp requests (type 13) and replies (type 14).

CVE: CVE−1999−0524

TestID: 811

16. SMB Log In Succeeded
Hosts affected: 192.168.4.122 (port: general/tcp)

The supplied credentials of the user:
Username: administrator, Password: *****, Domain: MSHOME

Allowed to logon to the remote server, these credentials will be used to access shares, the registry, etc.

TestID: 9219

17. Local Users Information: User Passwords That Never Expires
Hosts affected: 192.168.4.122 (port: general/tcp)

Using the supplied credentials it was possible to extract the list of local users whose password never expires. It is recommanded to allow/force users to change their password for security reasons.

Administrator
Guest
HelpAssistant
SUPPORT_388945a0
Support

Possible Solution: You should encourage your users to change passwords periodically.

TestID: 1676

18. Software Enumeration (Registry)
Hosts affected: 192.168.4.122 (port: microsoft−ds (445/tcp))

This test lists software installed on the remote host by crawling the registry entries in:
HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall

The following software are installed on the remote host:
1.0.0.9 [version]
VMware Tools [version 3.00.0000]
WebFldrs XP [version 9.50.7523]
Microsoft Script Debugger [version]
beSTORM 2.7.0 [version 2.7.0]

TestID: 9557

19. Remote Host Replies to SYN+FIN
Hosts affected: 192.168.4.122 (port: general/tcp)

The remote host does not discard TCP SYN packets that have the FIN flag set. If you are using a firewall, an attacker may use this flaw to bypass its rules.

For More Information:
http://www.kb.cert.org/vuls/id/464113

TestID: 2437

20. NetBIOS Information Retrieval
Hosts affected: 192.168.4.122 (port: netbios−ns (137/udp))

We tried to use NetBIOS over TCP/IP to find information about your computer. The following information was retrieved:
The following 6 NetBIOS names have been gathered :
SECURITY−5FF191 = This is the computer name registered for workstation services by a WINS client.
SECURITY−5FF191 = Computer name
MSHOME = Workgroup / Domain name
MSHOME = Workgroup / Domain name (part of the Browser elections)
MSHOME
__MSBROWSE__
The remote host has the following MAC address on its adapter :
00:0c:29:74:c6:ff

Impact: If NetBIOS is enabled and open to the outside, attackers may try to reach shared directories and files. This also gives sensitive information to the attacker such as the computer name, domain, or workgroup.

Possible Solution: The recommended solution is to block it in your firewall (or even your router, using ACLs). If you have 2 network interfaces, remove the binding for 'disk and printer' sharing from the external network interface.

For your general information, here is how to disable NetBIOS:
http://www.securiteam.com/windowsntfocus/3E5PUR5QAY.html

CVE: CAN−1999−0621

TestID: 838

Host Information	
Information about host 192.168.4.122	
Guessed Platform	Windows 5.1 *
MAC	00:0C:29:74:C6:FF (VMware)
NetBIOS Information	Manager: Windows 2000 LAN Manager Os: Windows 5.1 Domain: SECURITY−5FF191

NetBIOS Hostname:	SECURITY−5FF191
The following services were identified:	
msrpc (135/tcp)	Port open
netbios−ns (137/udp)	Port open
microsoft−ds (445/tcp)	Port open
ntp (123/udp)	Port open
netbios−ssn (139/tcp)	Port open

About vulnerability classification

Vulnerabilities in the report are classified into 3 categories: high, medium or low. This classification is based on industry standards and is endorsed by the major credit card companies. The following is the categories definitions:

High risk vulnerabilities are defined as being in one or more of the following categories: Backdoors, full Read/Write access to files, remote Command Execution, Potential Trojan Horses, or critical Information Disclosure (e.g. passwords).

Medium risk vulnerabilities are vulnerabilities that are not categorized as high risk, and belong to one or more of the following categories: Limited Access to files on the host, Directory Browsing and Traversal, Disclosure of Security Mechanisms (Filtering rules and security mechanisms), Denial of service, Unauthorized use of services (e.g. Mail relay).

Low risk vulnerabilities are those that do not fall in the "high" or "medium categories. Specifically, those will usually be: Sensitive information gathered on the server's configuration, Informative tests.

Host information − provided by different tests that discover informatio n about the target host, results of those test are not classified as vulnerabilities.

Guessed Platform − Detection of the operation system running on the host, via TCP/IP Stack FingerPrinting, this test is not very accurate, thus it is guessing.

What Next?

Knowing is just half the battle. Now you have to go and fix the problems we reported above. Intelligence gathering attacks may give attackers a good lead when trying to break into your host. Denial−of−Service attacks are much more dangerous than they seem at first glance, for more information take a look at: http://www.securiteam.com/securitynews/2JUQ6QAQTE.html

High Risk vulnerabilities should be dealt with immediately. They give an attacker almost immediate access to your system! This is also a good time to review your logs and see if you could have identified this scan if it was performed without your knowledge. Conduct these penetration tests periodically to check for the newest attacks.