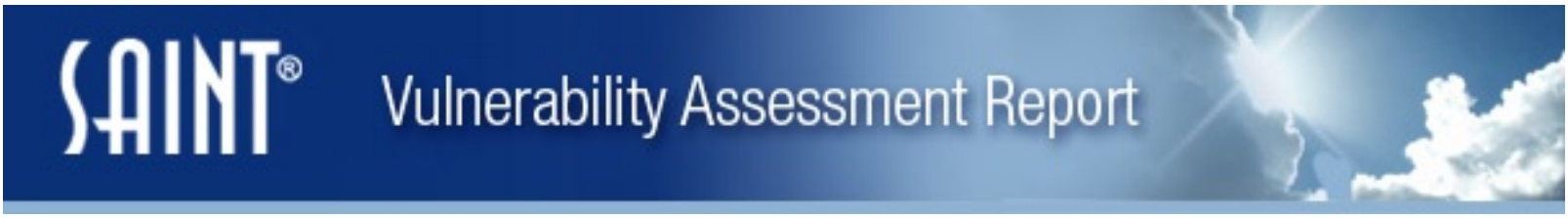


SOX Vulnerability Assessment Report

Report Generated: February 6, 2012

1.0 Background

The Sarbanes-Oxley Act (SOX) holds corporate executives accountable for the information reported on key financial statements, and has made it mandatory for organizations to ensure their financial information is accurate, and systems generating the information are secure and reliable. This means developing policies and practices that ensure proper access controls, implementing effective patch management of financial systems and related architecture, and conducting vulnerability assessments and remediation activities to continuously monitor risk to target systems and content.

2.0 Introduction

On February 3, 2012, at 9:07 AM, a SOX vulnerability assessment was conducted using the SAINT 7.11.17 vulnerability scanner. The results in the Summary section below document the findings from this scan, to include details about the host, vulnerabilities found, and Common Vulnerability Scoring System (CVSS) numerical score. This scan discovered a total of one live host and detected 56 critical problems, 164 areas of concern and 99 potential problems. The Summary and Details sections provide comprehensive information related to the vulnerabilities - to include content to assess risk and determine remediation.

This vulnerability scan and assessment where executed to support the organization's overall internal risk management practices, as well as facilitate provisions in Section 404 of the Sarbanes-Oxley Act, requiring management report annually on the effectiveness of internal controls for financial reporting and that external auditors confirm management's assessment.

3.0 Summary

The following vulnerability severity levels are used to categorize the vulnerabilities:

CRITICAL PROBLEMS
Vulnerabilities which pose an immediate threat to the network by allowing a remote attacker to directly gain read or write access, execute commands on the target, or create a denial of service.

AREAS OF CONCERN
Vulnerabilities which do not directly allow remote access, but do allow privilege elevation attacks, attacks on other targets using the vulnerable host as an intermediary, or gathering of passwords or configuration information which could be used to plan an attack.

POTENTIAL PROBLEMS
Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.

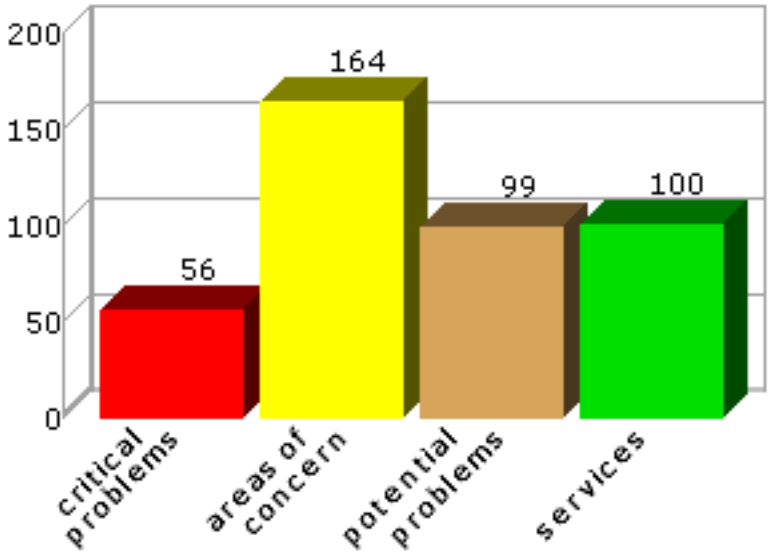
SERVICES

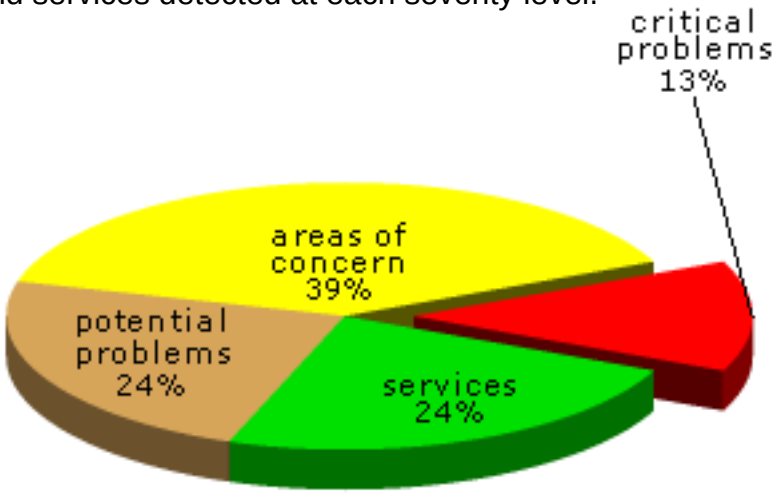
Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The sections below summarize the results of the scan.

3.1 Vulnerabilities by Severity

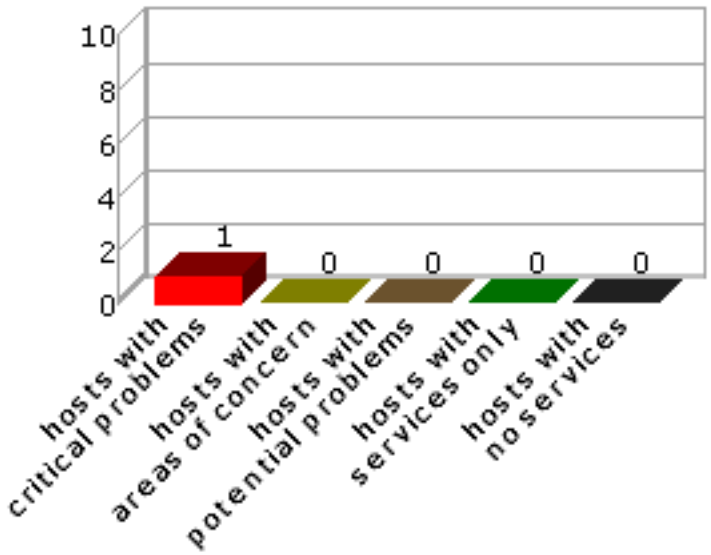
This section shows the overall number of vulnerabilities and services detected at each severity level.





3.2 Hosts by Severity

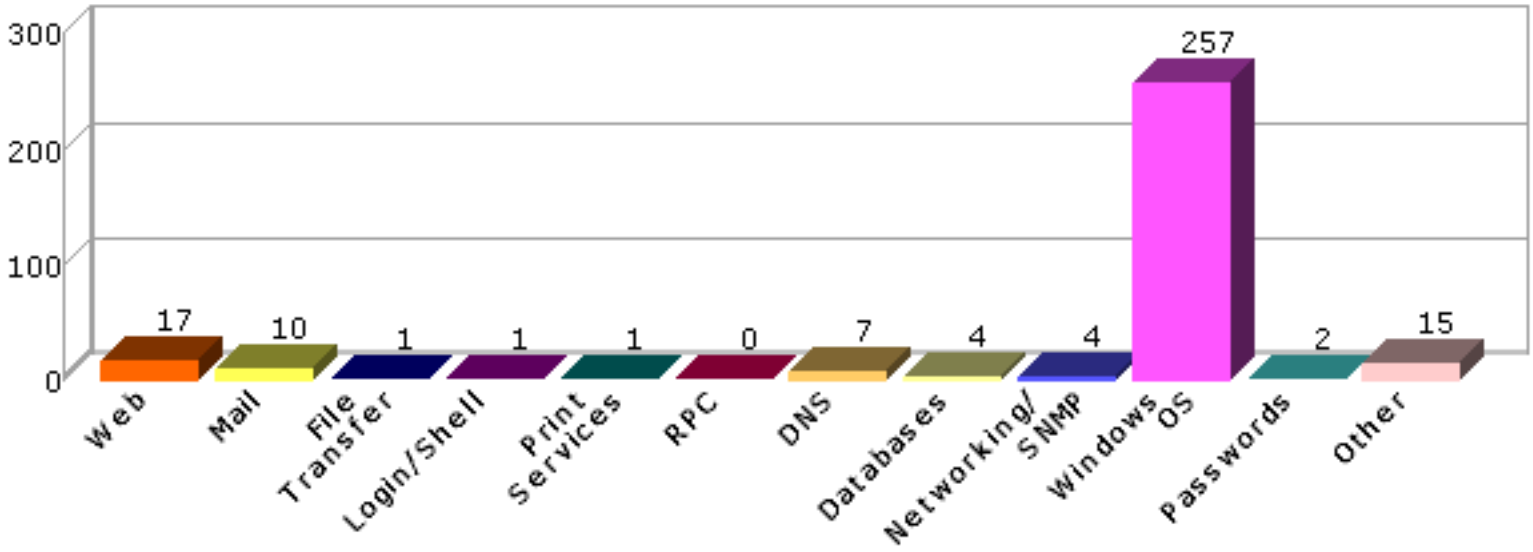
This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.

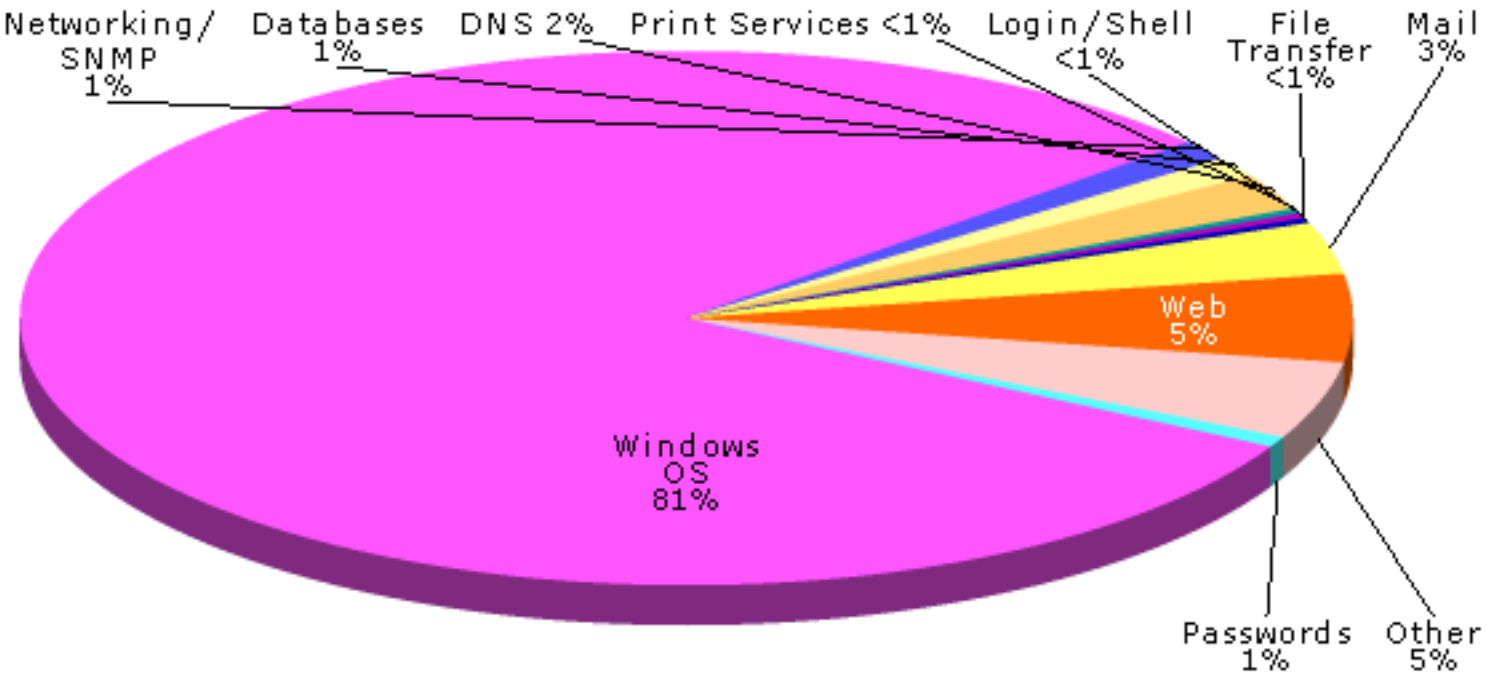


3.3 Vulnerabilities by Class

This section shows the number of vulnerabilities detected in each of the following classes.

Class	Description
Web	Vulnerabilities in web servers, CGI programs, and any other software offering an HTTP interface
Mail	Vulnerabilities in SMTP, IMAP, POP, or web-based mail services
File Transfer	Vulnerabilities in FTP and TFTP services
Login/Shell	Vulnerabilities in ssh, telnet, rlogin, rsh, or rexec services
Print Services	Vulnerabilities in lpd and other print daemons
RPC	Vulnerabilities in Remote Procedure Call services
DNS	Vulnerabilities in Domain Name Services
Databases	Vulnerabilities in database services
Networking/SNMP	Vulnerabilities in routers, switches, firewalls, or any SNMP service
Windows OS	Missing hotfixes or vulnerabilities in the registry or SMB shares
Passwords	Missing or easily guessed user passwords
Other	Any vulnerability which does not fit into one of the above classes





4.0 Overview

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

4.1 Host List

This table presents an overview of the hosts discovered on the network.

Host Name	Netbios Name	IP Address	Host Type	Critical Problems	Areas of Concern	Potential Problems
win2k	SAINTLAB02	10.7.0.2	Windows 2000 SP2	56	164	99

4.2 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Severity	Vulnerability / Service	Class	CVE	Exploit Available?
win2k	critical	Active Directory LDAP request memory allocation vulnerability	Windows OS	CVE-2008-4023	no
win2k	critical	Active Directory Remote Code Execution MS09-018	Windows OS	CVE-2009-1139	no
win2k	critical	Buffer overflow in Active Directory	Windows OS	CVE-2003-0507	no
win2k	critical	Windows Active Directory additional denial of service	Windows OS	CVE-2008-0088	no
win2k	critical	Windows Active Directory denial of service	Windows OS	CVE-2007-3028	no
win2k	critical	Windows Active Directory denial of service MS08-035	Windows OS	CVE-2008-1445	no
win2k	critical	Windows Active Directory denial of service MS09-066	Windows OS	CVE-2009-1928	no
win2k	critical	Windows Active Directory remote code execution	Windows OS	CVE-2007-0040	no
win2k	critical	Guessed password to windows account (kline:kline)	Passwords	CVE-1999-0503 CVE-1999-0505	yes
win2k	critical	Guessed password to windows account (testadmin:testadmin)	Passwords	CVE-1999-0503 CVE-1999-0505	yes
win2k	critical	Folder traversal in IIS (Double Decoding)	Web	CVE-2001-0333	yes
win2k	critical	IPP Service integer overflow	Web	CVE-2008-1446	no
win2k	critical	multiple vulnerabilities in IIS 5.0	Web	CVE-2002-0071 CVE-2002-0072 CVE-2002-0073 CVE-2002-0074 CVE-2002-0075 CVE-2002-0079 CVE-2002-0147 CVE-2002-0148 CVE-2002-0149 CVE-2002-0150	yes
win2k	critical	Microsoft Internet Information Services FTP Server Remote Buffer Overflow	Windows OS	CVE-2009-2521 CVE-2009-3023	yes
win2k	critical	WebDAV XML message handler denial of service	Web	CVE-2003-0718	no

win2k	critical	buffer overflow in IIS 5.0 WebDAV	Web	CVE-2001-0241 CVE-2001-0500 CVE-2003-0109	yes
win2k	critical	Microsoft mail server vulnerabilities, smtpsvc.dll dated 2001-5-4	Mail	CVE-2010-0024 CVE-2010-0025 CVE-2010-1689 CVE-2010-1690	no
win2k	critical	denial of service in Windows SMTP service	Mail	CVE-2002-0055 CVE-2003-1106	no
win2k	critical	vulnerable Microsoft NNTP version: 5.0.2195.2966	Other	CVE-2004-0574	no
win2k	critical	SQL Server account sa has no password	Databases	CVE-2000-1209	no
win2k	critical	Windows DNS Server RPC Management Interface Buffer Overflow	DNS	CVE-2007-1748	yes
win2k	critical	Windows Kerberos vulnerability	Other	CVE-2005-1981 CVE-2005-1982	no
win2k	critical	Windows Kerberos vulnerability (MS10-014)	Other	CVE-2005-1981 CVE-2005-1982 CVE-2010-0035	no
win2k	critical	vulnerability in Windows Locator service	Windows OS	CVE-2003-0003	no
win2k	critical	vulnerability in Windows Media Services (nsiislog.dll)	Web	CVE-2003-0227 CVE-2003-0349	no
win2k	critical	Windows Plug and Play vulnerability	Windows OS	CVE-2005-1983	yes
win2k	critical	Windows print spooler vulnerability	Print Services	CVE-2005-1984	no
win2k	critical	Windows SNMP buffer overflow	Networking /SNMP	CVE-2006-5583	no
win2k	critical	Distributed Transaction Coordinator Denial of Service	Windows OS	CVE-2006-0034 CVE-2006-1184	no
win2k	critical	Microsoft Windows Message Queuing Service Queue Name Handling Memory Corruption	Windows OS	CVE-2008-3479	no
win2k	critical	Multiple Windows vulnerabilities (ms04-011)	Windows OS	CVE-2003-0533 CVE-2003-0663 CVE-2003-0719 CVE-2003-0806 CVE-2003-0906 CVE-2003-0907 CVE-2003-0908 CVE-2003-0909 CVE-2003-0910 CVE-2004-0117 CVE-2004-0118 CVE-2004-0119 CVE-2004-0120 CVE-2004-0123	yes
win2k	critical	Multiple buffer overflows in SMB	Windows OS	CVE-2008-4114 CVE-2008-4834 CVE-2008-4835	no
win2k	critical	RPC runtime library vulnerability	Windows OS	CVE-2003-0807 CVE-2003-0813 CVE-2004-0116 CVE-2004-0124	no
win2k	critical	Win2000 RPCSS buffer overflow	Windows OS	CVE-2003-0528 CVE-2003-0605 CVE-2003-0715	no
win2k	critical	Windows 2000 ASN1 buffer overflow	Windows OS	CVE-2003-0818	no
win2k	critical	Windows 2000 RPC buffer overflow	Windows OS	CVE-2003-0352	yes

win2k	critical	Windows COM+ command execution vulnerability	Windows OS	CVE-2005-1978 CVE-2005-1979 CVE-2005-1980 CVE-2005-2119	no
win2k	critical	Windows DNS Resolution Remote Code Execution	Windows OS	CVE-2006-3440 CVE-2006-3441	no
win2k	critical	Windows Mailslot heap overflow	Windows OS	CVE-2006-1314 CVE-2006-1315	no
win2k	critical	Windows Media Unicast Service transport information buffer overflow	Windows OS	CVE-2010-0478	yes
win2k	critical	Windows Message Queuing validation vulnerability	Windows OS	CVE-2007-3039	yes
win2k	critical	Windows RPC authentication denial of service	Windows OS	CVE-2007-2228	no
win2k	critical	Windows SMB Transaction response buffer overflow	Windows OS	CVE-2005-0045	no
win2k	critical	Windows SMB input validation vulnerability	Windows OS	CVE-2005-1206	no
win2k	critical	Windows SMB invalid handle denial of service	Windows OS	CVE-2006-2373 CVE-2006-2374	no
win2k	critical	Windows Server Service Buffer Overrun	Windows OS	CVE-2006-3439	yes
win2k	critical	Windows Server Service MS08-067 buffer overflow	Windows OS	CVE-2008-4250	yes
win2k	critical	Windows TCP/IP vulnerabilities	Windows OS	CVE-2004-0230 CVE-2004-0790 CVE-2004-1060 CVE-2005-0048 CVE-2005-0688	no
win2k	critical	Windows WMF gdi32.dll vulnerability	Windows OS	CVE-2005-4560	yes
win2k	critical	Windows Workstation service remote code execution	Windows OS	CVE-2006-4691	yes
win2k	critical	Windows messenger service buffer overflow	Windows OS	CVE-2003-0717	no
win2k	critical	Windows print spooler vulnerabilities	Windows OS	CVE-2009-0228 CVE-2009-0229 CVE-2009-0230	yes
win2k	critical	Windows server driver denial of service	Windows OS	CVE-2006-3942 CVE-2006-4696	no
win2k	critical	Windows workstation service buffer overflow	Windows OS	CVE-2003-0812	no
win2k	critical	vulnerable version of SMB Server (MS10-012) dated 2001-5-8	Windows OS	CVE-2010-0020 CVE-2010-0021 CVE-2010-0022 CVE-2010-0231	no
win2k	critical	WINS Could Allow Remote Code Execution	Windows OS	CVE-2009-1923 CVE-2009-1924	no
win2k	concern	ASP.NET application folder information disclosure	Web	CVE-2006-1300	no
win2k	concern	Web server allows cross-site tracing	Web		no
win2k	concern	Windows DNS server allows cache poisoning	DNS	CVE-2001-1452	no
win2k	concern	DNS cache snooping vulnerability	DNS		no
win2k	concern	DNS server allows zone transfers	DNS	CVE-1999-0532	yes
win2k	concern	Microsoft IIS ASP Upload Command Execution vulnerability	Web	CVE-2006-0026	no

win2k	concern	Vulnerabilities in IIS 5.0	Web	CVE-2000-0770 CVE-2001-0151 CVE-2001-0241 CVE-2001-0500 CVE-2001-0507 CVE-2002-0869 CVE-2002-1180 CVE-2002-1181 CVE-2002-1182 CVE-2003-0223 CVE-2003-0224 CVE-2003-0225 CVE-2003-0226	yes
win2k	concern	Microsoft IIS Authentication Method Disclosed	Web		no
win2k	concern	IIS file update notification privilege elevation	Windows OS	CVE-2008-0074	no
win2k	concern	Microsoft IIS WebDAV Request Directory Security Bypass	Web	CVE-2009-1122 CVE-2009-1535	no

win2k	concern	Internet Explorer 5 vulnerable version, mshtml.dll dated 2001-5-8	Windows OS	CVE-2006-4697 CVE-2007-0217 CVE-2007-0218 CVE-2007-0219 CVE-2007-0942 CVE-2007-0943 CVE-2007-0944 CVE-2007-0945 CVE-2007-1091 CVE-2007-1751 CVE-2007-2216 CVE-2007-2221 CVE-2007-2222 CVE-2007-3027 CVE-2007-3041 CVE-2007-3826 CVE-2007-3892 CVE-2007-3893 CVE-2007-3902 CVE-2007-4790 CVE-2008-0076 CVE-2008-0078 CVE-2008-1085 CVE-2008-1544 CVE-2008-2255 CVE-2008-2256 CVE-2008-2257 CVE-2008-2258 CVE-2008-2947 CVE-2008-3476 CVE-2008-4261 CVE-2008-4844 CVE-2009-0550 CVE-2009-0552 CVE-2009-0554 CVE-2009-1140 CVE-2009-1547 CVE-2009-1918 CVE-2009-1919 CVE-2009-2493 CVE-2009-2529 CVE-2010-0247 CVE-2010-0255 CVE-2010-0488 CVE-2010-0489 CVE-2010-0491 CVE-2010-0805	yes
win2k	concern	Internet Explorer 5 vulnerable version, wininet.dll dated 2001-5-8	Windows OS	CVE-2007-1692	no
win2k	concern	Internet Explorer ADODB.Connection ActiveX Object Memory Corruption	Windows OS	CVE-2006-5559	no
win2k	concern	Internet Explorer August 2006 CSU fixes	Windows OS	CVE-2004-1166 CVE-2006-3280 CVE-2006-3450 CVE-2006-3451 CVE-2006-3637 CVE-2006-3638 CVE-2006-3639 CVE-2006-3640	no
win2k	concern	Internet Explorer COM Objects Instantiation vulnerability	Windows OS	CVE-2006-4193 CVE-2006-4219	no

win2k	concern	Internet Explorer COM object memory corruption	Windows OS	CVE-2005-2127	no
win2k	concern	Internet Explorer Cascading Style Sheets vulnerability	Windows OS	CVE-2004-0216 CVE-2004-0727 CVE-2004-0839 CVE-2004-0841 CVE-2004-0842 CVE-2004-0843 CVE-2004-0844 CVE-2004-0845	no
win2k	concern	Internet Explorer Create Text Range code injection	Windows OS	CVE-2006-1185 CVE-2006-1186 CVE-2006-1188 CVE-2006-1189 CVE-2006-1190 CVE-2006-1191 CVE-2006-1192 CVE-2006-1245 CVE-2006-1359 CVE-2006-1388	yes
win2k	concern	Internet Explorer DHTML method memory corruption	Windows OS	CVE-2005-0053 CVE-2005-0054 CVE-2005-0055 CVE-2005-0056	no
win2k	concern	Internet Explorer December 2006 CSU fixes	Windows OS	CVE-2006-5577 CVE-2006-5578 CVE-2006-5579 CVE-2006-5581	no
win2k	concern	Internet Explorer DirectAnimation overflow	Windows OS	CVE-2006-4446 CVE-2006-4687 CVE-2006-4777 CVE-2006-5884	no
win2k	concern	Internet Explorer Exception Handling Memory Corruption vulnerability	Windows OS	CVE-2005-4089 CVE-2006-1303 CVE-2006-1626 CVE-2006-2218 CVE-2006-2382 CVE-2006-2383 CVE-2006-2384 CVE-2006-2385	no
win2k	concern	Internet Explorer JPEG buffer overflow	Windows OS	CVE-2005-1988 CVE-2005-1989 CVE-2005-1990	yes
win2k	concern	Internet Explorer JS remote code execution	Windows OS	CVE-2006-1313	no
win2k	concern	Internet Explorer JS stack overflow	Windows OS	CVE-2006-0753 CVE-2006-0830	no
win2k	concern	Internet Explorer JavaScript vulnerability	Windows OS	CVE-2005-1790 CVE-2005-2829 CVE-2005-2830 CVE-2005-2831	yes
win2k	concern	Internet Explorer Nested OBJECT tag memory corruption	Windows OS	CVE-2006-1992 CVE-2006-2094 CVE-2006-2111	no
win2k	concern	Internet Explorer PNG buffer overflow	Windows OS	CVE-2002-0648 CVE-2005-1211	no
win2k	concern	Internet Explorer URL parsing buffer overflow	Windows OS	CVE-2005-0553 CVE-2005-0554 CVE-2005-0555	yes
win2k	concern	Internet Explorer VBScript and JScript decoding vulnerability	Windows OS	CVE-2008-0083	no

win2k	concern	Internet Explorer VML Remote Code Execution	Windows OS	CVE-2006-4868	yes
win2k	concern	Internet Explorer VML buffer overflow (MS07-004)	Windows OS	CVE-2007-0024	yes
win2k	concern	Internet Explorer WMF handling vulnerability	Windows OS	CVE-2006-0020	no
win2k	concern	Internet Explorer vulnerable VML version dated 2001-5-8	Windows OS	CVE-2007-1749 CVE-2011-1266	no
win2k	concern	Jscript.dll buffer overflow vulnerability	Windows OS	CVE-2009-1920	no
win2k	concern	Windows 2000 IE6 VML vulnerable version, vgx.dll dated 2001-5-8	Windows OS	CVE-2007-5348 CVE-2008-3012 CVE-2008-3013 CVE-2008-3014	no
win2k	concern	Windows 2000 License Logging Server vulnerability	Windows OS	CVE-2009-2523	no
win2k	concern	vulnerability in License Logging Service	Windows OS	CVE-2005-0050	no
win2k	concern	WordPerfect Converter buffer overflow	Windows OS	CVE-2004-0573	no
win2k	concern	Microsoft outlook ATL vulnerability (MS09-037)	Windows OS	CVE-2008-0015 CVE-2008-0020 CVE-2009-0901 CVE-2009-2493 CVE-2009-2494	yes
win2k	concern	Outlook Express Could Allow Remote Code Execution (MS10-030)	Windows OS	CVE-2010-0816	no
win2k	concern	Windows MHTML protocol handler vulnerability	Windows OS	CVE-2008-1448	no
win2k	concern	Microsoft SQL Server vulnerable version, sqlservr.exe dated 2000-8-6	Databases	CVE-2007-5348 CVE-2008-3012 CVE-2008-3013 CVE-2008-3014 CVE-2008-3015	no

win2k	concern	Microsoft SQL Server vulnerable version: 8.00.194	Databases	CVE-1999-0999 CVE-2000-0199 CVE-2000-0202 CVE-2000-0402 CVE-2000-0485 CVE-2000-0603 CVE-2000-1081 CVE-2000-1082 CVE-2000-1083 CVE-2000-1084 CVE-2000-1085 CVE-2000-1086 CVE-2000-1087 CVE-2000-1088 CVE-2001-0344 CVE-2001-0542 CVE-2001-0879 CVE-2002-0056 CVE-2002-0154 CVE-2002-0186 CVE-2002-0187 CVE-2002-0624 CVE-2002-0641 CVE-2002-0642 CVE-2002-0644 CVE-2002-0645 CVE-2002-0695 CVE-2002-0721 CVE-2002-0859 CVE-2002-0982 CVE-2002-1123 CVE-2002-1137 CVE-2002-1138 CVE-2002-1145 CVE-2003-0230 CVE-2003-0231 CVE-2003-0232	yes
win2k	concern	Telnet Authentication Reflection	Login/Shell	CVE-2009-1930	yes
win2k	concern	Outlook Express Contact Record vulnerability	Mail	CVE-2006-2386	no
win2k	concern	Outlook Express Windows Address Book vulnerability	Mail	CVE-2006-0014	no
win2k	concern	Outlook Express vulnerable version, inetcomm.dll dated 2001-5-8	Mail	CVE-2006-2111 CVE-2007-2225 CVE-2007-2227 CVE-2007-3897	no
win2k	concern	Microsoft VB6 FlexGrid ActiveX control vulnerable version dated 1999-9-7	Other	CVE-2008-4253	no
win2k	concern	null session access using alternate pipes	Windows OS	CVE-2005-2150	no
win2k	concern	Windows DNS lack of entropy spoofing attack	DNS	CVE-2007-3898	no
win2k	concern	Windows DNS service allows spoofing	DNS	CVE-2009-0093 CVE-2009-0233 CVE-2009-0234	no
win2k	concern	Windows Plug and Play privilege elevation	Windows OS	CVE-2005-2120	no
win2k	concern	Schedule key allows write access	Windows OS	CVE-1999-0589	no
win2k	concern	Windows telephony service vulnerability	Windows OS	CVE-2005-0058	yes
win2k	concern	Blended threat privilege elevation vulnerability	Windows OS	CVE-2008-2540	no
win2k	concern	DirectShow buffer overflow	Windows OS	CVE-2005-2128	no

win2k	concern	DirectX SAMI-MJPEG parsing remote code execution for DirectX 7.0	Windows OS	CVE-2008-1444	no
win2k	concern	DirectX parsing remote code execution for DirectX 7.0	Windows OS	CVE-2007-3895 CVE-2007-3901	yes
win2k	concern	Elevation of Privilege Vulnerabilities in Windows (MS09-012)	Windows OS	CVE-2008-1436 CVE-2009-0078	no
win2k	concern	Elevation of Privilege Vulnerabilities in Windows (MS10-015)	Windows OS	CVE-2010-0232 CVE-2010-0233	no
win2k	concern	HTML Application Host vulnerability in Windows shell	Windows OS	CVE-2005-0063	no
win2k	concern	HTML Help cross-domain vulnerability	Windows OS	CVE-2004-1043	no
win2k	concern	Jet Database Engine vulnerable version, msjet40.dll dated 2001-5-8	Windows OS	CVE-2005-0944 CVE-2007-6026 CVE-2008-1092	yes
win2k	concern	Kodak Image Viewer remote code execution	Windows OS	CVE-2007-2217	yes
win2k	concern	Microsoft Agent ACF memory corruption	Windows OS	CVE-2006-3445	no
win2k	concern	Microsoft Agent URL parsing vulnerability	Windows OS	CVE-2007-1205	no
win2k	concern	Microsoft Agent vulnerable version, agentdpv.dll dated 2001-5-8	Windows OS	CVE-2007-3040	yes
win2k	concern	Microsoft Color Management Module buffer overflow	Windows OS	CVE-2005-1219	yes
win2k	concern	Microsoft Data Access Component vulnerability	Windows OS	CVE-2006-0003	yes
win2k	concern	Microsoft DirectShow Quartz AVI buffer overflow	Windows OS	CVE-2010-0250	no
win2k	concern	Microsoft DirectShow QuickTime Movie Parsing Code Execution	Windows OS	CVE-2009-1537 CVE-2009-1538 CVE-2009-1539	yes
win2k	concern	Microsoft Image Color Management System vulnerable version, mscms.dll dated 2001-5-8	Windows OS	CVE-2008-2245	no
win2k	concern	Microsoft Paint Integer Overflow vulnerability	Windows OS	CVE-2010-0028	no
win2k	concern	Microsoft Windows DHTML remote code execution vulnerability (MS09-046)	Windows OS	CVE-2009-2519	no
win2k	concern	Microsoft Windows vulnerable version, msconv97.dll dated 2001-5-8	Windows OS	CVE-2009-2506	no
win2k	concern	Multiple GDI vulnerabilities fixed by MS07-017	Windows OS	CVE-2006-5586 CVE-2006-5758 CVE-2007-0038 CVE-2007-1211 CVE-2007-1212 CVE-2007-1213 CVE-2007-1215	yes
win2k	concern	NetBIOS Name Service information disclosure	Windows OS	CVE-2003-0661	no
win2k	concern	RTF MFC component memory corruption	Windows OS	CVE-2007-0025	no
win2k	concern	RTF OLE dialog memory corruption	Windows OS	CVE-2007-0026	no
win2k	concern	RTF RichEdit component memory corruption	Windows OS	CVE-2006-1311	no
win2k	concern	Vulnerability in Message Queuing Could Allow Elevation of Privilege	Windows OS	CVE-2009-1922	no
win2k	concern	Vulnerability in the OpenType Compact Font Format Driver Could Allow Elevation of Privilege	Windows OS	CVE-2010-0819	no
win2k	concern	Vulnerable ActiveX Control enabled (MS11-090)	Windows OS	CVE-2011-3397	no

win2k	concern	Vulnerable MFC Library FileFind Class file mfc42.dll	Windows OS	CVE-2007-4916	no
win2k	concern	Vulnerable MFC Library FileFind Class file mfc42u.dll	Windows OS	CVE-2007-4916	no
win2k	concern	Win32 API parameter validation vulnerability	Windows OS	CVE-2007-2219	no
win2k	concern	Windows 2000 GDI vulnerable version, gdi32.dll dated 2001-5-8	Windows OS	CVE-2008-1083 CVE-2008-1087 CVE-2008-2249 CVE-2008-3465	yes
win2k	concern	Windows 2000 Kernel Debugger buffer overflow	Windows OS	CVE-2003-0112	no
win2k	concern	Windows 2000 Utility Manager privilege elevation	Windows OS	CVE-2004-0213	no
win2k	concern	Windows ASN1 spoofing vulnerability	Windows OS	CVE-2009-2510 CVE-2009-2511	no
win2k	concern	Windows Authenticode Signature Verification (MS10-019) version, wintrust.dll dated 2001-5-8	Windows OS	CVE-2010-0486	no
win2k	concern	Windows CSRSS Local (MS10-011) vulnerable version, csrsrv.dll dated 2001-5-8	Windows OS	CVE-2010-0023	no
win2k	concern	Windows CSRSS remote code execution	Windows OS	CVE-2006-6696 CVE-2006-6797	no
win2k	concern	Windows Cabinet File Viewer (MS10-019) version, cabview.dll dated 2001-5-8	Windows OS	CVE-2010-0487	no
win2k	concern	Windows DHCP Client buffer overflow	Windows OS	CVE-2006-2372	no
win2k	concern	Windows DHTML Editing Component vulnerability	Windows OS	CVE-2004-1319	no
win2k	concern	Windows DNS Client Spoofing vulnerability (MS08-037)	Windows OS	CVE-2008-1447	no
win2k	concern	Windows DNS Resolution Vulnerability	Windows OS	CVE-2011-0657	no
win2k	concern	Windows DNS Server Spoofing vulnerability (MS08-037)	Windows OS	CVE-2008-1447 CVE-2008-1454	no
win2k	concern	Windows DNS Spoofing vulnerability	Windows OS	CVE-2008-0087	no
win2k	concern	Windows DirectShow AVI Filter buffer overflow	Windows OS	CVE-2010-0250	no
win2k	concern	Windows EMF/WMF image file vulnerability	Windows OS	CVE-2005-0803 CVE-2005-2123 CVE-2005-2124	no
win2k	concern	Windows Embedded OpenType Font Engine Vulnerability	Windows OS	CVE-2010-0018	no
win2k	concern	Windows Embedded OpenType Font Engine vulnerabilities	Windows OS	CVE-2009-0231 CVE-2009-0232	no
win2k	concern	Windows Explorer COM object command execution	Windows OS	CVE-2004-2289 CVE-2006-0012	no
win2k	concern	Windows Explorer Web View command execution	Windows OS	CVE-2005-1191	no
win2k	concern	Windows Explorer setslice remote code execution	Windows OS	CVE-2006-3730	yes
win2k	concern	Windows GDI image handling buffer overflow	Windows OS	CVE-2007-3034	no
win2k	concern	Windows HTML Help integer overflow	Windows OS	CVE-2005-1208	no
win2k	concern	Windows Help File Handling Heap Buffer Overflow	Windows OS	CVE-2007-1912	no
win2k	concern	Windows Help File Image Processing Heap Buffer Overflow	Windows OS	CVE-2006-1591	no
win2k	concern	Windows Hyperlink Object Library buffer overflow	Windows OS	CVE-2005-0057	no

win2k	concern	Windows Hyperlink Object Library function vulnerability	Windows OS	CVE-2006-3086 CVE-2006-3438	yes
win2k	concern	Windows Internet Authentication Service vulnerabilities	Windows OS	CVE-2009-3677	no
win2k	concern	Windows Kernel privilege elevation (ms06-049) vulnerability	Windows OS	CVE-2006-3444	no
win2k	concern	Windows Kernel privilege elevation (ms07-022) vulnerability	Windows OS	CVE-2007-1206	no
win2k	concern	Windows Kernel privilege elevation vulnerability	Windows OS	CVE-2005-2827	no
win2k	concern	Windows LSASS IPSEC Denial-of-Service Vulnerability	Windows OS	CVE-2009-3675	no
win2k	concern	Windows LSASS vulnerability	Windows OS	CVE-2007-5352	no
win2k	concern	Windows ListBox and ComboBox buffer overflow	Windows OS	CVE-2003-0659	no
win2k	concern	Windows MMC redirect cross-site scripting vulnerability	Windows OS	CVE-2006-3643	no
win2k	concern	Windows MPEG layer 3 codec vulnerable version, l3codecx.ax dated 2001-5-8	Windows OS	CVE-2010-0480	no
win2k	concern	Windows Media Format ASF file parsing vulnerability	Windows OS	CVE-2007-0064	no
win2k	concern	Windows Media Player ASF file heap overflow	Windows OS	CVE-2009-2527	no
win2k	concern	Windows Media Player plug-in EMBED vulnerability	Windows OS	CVE-2006-0005	yes
win2k	concern	Windows Media components SPN credential reflection vulnerability	Windows OS	CVE-2008-3009 CVE-2008-3010	no
win2k	concern	Windows Media decompression vulnerabilities	Windows OS	CVE-2010-1879 CVE-2010-1880	no
win2k	concern	Windows Metafile rendering buffer overflow	Windows OS	CVE-2004-0207 CVE-2004-0208 CVE-2004-0209 CVE-2004-0211	yes
win2k	concern	Windows OLE Automation remote code execution vulnerability	Windows OS	CVE-2007-0065 CVE-2007-2224	no
win2k	concern	Windows OLE input validation vulnerability	Windows OS	CVE-2005-0044 CVE-2005-0047	no
win2k	concern	Windows POSIX subsystem buffer overflow	Windows OS	CVE-2004-0210	no
win2k	concern	Windows RPC Marshalling Engine vulnerability	Windows OS	CVE-2009-0568	no
win2k	concern	Windows SMB Client vulnerabilities (MS10-006)	Windows OS	CVE-2010-0016	no
win2k	concern	Windows SMB Client vulnerabilities (MS10-020)	Windows OS	CVE-2009-3676 CVE-2010-0269 CVE-2010-0270 CVE-2010-0476 CVE-2010-0477	no
win2k	concern	Windows SMB Remote Code Execution	Windows OS	CVE-2008-4038	no
win2k	concern	Windows SMB credential reflection vulnerability	Windows OS	CVE-2008-4037	yes
win2k	concern	Windows Schannel digital signature parsing vulnerability	Windows OS	CVE-2007-2218	no
win2k	concern	Windows Schannel spoofing vulnerability	Windows OS	CVE-2009-0085	no
win2k	concern	Windows Services for UNIX setuid privilege elevation	Windows OS	CVE-2007-3036	no
win2k	concern	Windows Shell Handler vulnerability	Windows OS	CVE-2010-0027	no
win2k	concern	Windows VB script vulnerable version, vbscript.dll dated 2001-5-8	Windows OS	CVE-2010-0483 CVE-2011-0031	no

win2k	concern	Windows WMA Voice codec vulnerability	Windows OS	CVE-2009-0555 CVE-2009-2525	no
win2k	concern	Windows Web Fonts vulnerability	Windows OS	CVE-2006-0010	no
win2k	concern	Windows atl.dll vulnerable (MS09-037)	Windows OS	CVE-2008-0015 CVE-2008-0020 CVE-2009-0901 CVE-2009-2493 CVE-2009-2494	yes
win2k	concern	Windows cursor and icon vulnerabilities	Windows OS	CVE-2004-1049 CVE-2004-1305	yes
win2k	concern	Windows dhtmled.ocx vulnerable (MS09-037)	Windows OS	CVE-2008-0015 CVE-2008-0020 CVE-2009-0901 CVE-2009-2493 CVE-2009-2494	yes
win2k	concern	Windows event system subscription request and pointer array vulnerabilities	Windows OS	CVE-2008-1456 CVE-2008-1457	no
win2k	concern	Windows kernel GDI validation vulnerabilities	Windows OS	CVE-2009-0081 CVE-2009-0082 CVE-2009-0083	no
win2k	concern	Windows kernel access request buffer overflow	Windows OS	CVE-2005-0060 CVE-2005-0061 CVE-2005-0550 CVE-2005-0551	no
win2k	concern	Windows kernel and LSASS privilege elevation	Windows OS	CVE-2004-0893 CVE-2004-0894	no
win2k	concern	Windows kernel desktop validation vulnerabilities	Windows OS	CVE-2009-1123 CVE-2009-1124 CVE-2009-1125 CVE-2009-1126	no
win2k	concern	Windows kernel embedded font vulnerabilities	Windows OS	CVE-2009-1127 CVE-2009-2513 CVE-2009-2514	no
win2k	concern	Windows kernel multiple privilege elevation vulnerabilities (MS10-032)	Windows OS	CVE-2010-0484 CVE-2010-0485 CVE-2010-1255	no
win2k	concern	Windows kernel property validation vulnerabilities	Windows OS	CVE-2008-2250 CVE-2008-2251 CVE-2008-2252	no
win2k	concern	Windows kernel user mode callback vulnerability	Windows OS	CVE-2008-1084	no
win2k	concern	Windows kernel vulnerable (MS10-021) version, ntoskrnl.exe dated 2001-5-8	Windows OS	CVE-2010-0234 CVE-2010-0235 CVE-2010-0236 CVE-2010-0237 CVE-2010-0238 CVE-2010-0481 CVE-2010-0482 CVE-2010-0810	no
win2k	concern	Windows kernel vulnerable version, ntoskrnl.exe dated 2001-5-8	Windows OS	CVE-2009-2515 CVE-2009-2516 CVE-2009-2517	no
win2k	concern	Windows media file processing vulnerable (MS09-038)	Windows OS	CVE-2009-1545 CVE-2009-1546	no
win2k	concern	Windows shell drag-and-drop vulnerability	Windows OS	CVE-2005-0053	no
win2k	concern	Windows shortcut file command execution	Windows OS	CVE-2005-2117 CVE-2005-2118 CVE-2005-2122	no
win2k	concern	Windows unhandled exception vulnerability	Windows OS	CVE-2006-3443 CVE-2006-3648	no

win2k	concern	application start buffer overflow in Windows shell	Windows OS	CVE-2004-0214 CVE-2004-0572	no
win2k	concern	WINS local privilege elevation	Windows OS	CVE-2008-1451	no
win2k	potential	active scripting enabled in Internet zone for Administrator.SAINTLAB02	Web		no
win2k	potential	anonymous FTP is allowed	File Transfer	CVE-1999-0497	no
win2k	potential	AV Information: AntiVirus software not found (AVG F-Secure Forefront McAfee Symantec TrendMicro)	Other		no
win2k	potential	possible vulnerability in Apple Filing Protocol 2.0	Other	CVE-2004-0430	no
win2k	potential	Cookie Injection vulnerabilities in IE	Web	CVE-2004-0866 CVE-2004-0869	no
win2k	potential	The daytime service is running	Other	CVE-1999-0638	no
win2k	potential	The discard service is running	Other	CVE-1999-0636	no
win2k	potential	DNS server allows recursive queries	DNS		no
win2k	potential	The echo service is running	Other	CVE-1999-0635	no
win2k	potential	guessable read community string	Networking /SNMP	CVE-1999-0516 CVE-1999-0517	no
win2k	potential	IIS .HTR filter is enabled	Web	CVE-2002-0071 CVE-2002-0364	yes
win2k	potential	Cookie without HTTPOnly attribute can be accessed by scripts	Web		no
win2k	potential	ICMP timestamp requests enabled	Other	CVE-1999-0524	no
win2k	potential	Internet Explorer ADODB.Stream object enabled	Windows OS	CVE-2004-0985	no
win2k	potential	Internet Explorer Modal Dialog zone bypass	Windows OS	CVE-2003-1048 CVE-2004-0549 CVE-2004-0566	no
win2k	potential	Internet Explorer Shell.Explorer object enabled	Windows OS		no
win2k	potential	Internet Explorer Travel Log vulnerability	Windows OS	CVE-2003-1025 CVE-2003-1026 CVE-2003-1027	no
win2k	potential	Internet Explorer cross-domain vulnerabilities	Windows OS	CVE-2003-0814 CVE-2003-0815 CVE-2003-0816 CVE-2003-0817 CVE-2003-0823	no
win2k	potential	Internet Explorer patch needed	Windows OS	CVE-2003-0113 CVE-2003-0114 CVE-2003-0115 CVE-2003-0116 CVE-2003-0309 CVE-2003-0344 CVE-2003-0530 CVE-2003-0531 CVE-2003-0532 CVE-2003-0701 CVE-2003-0809 CVE-2003-0838 CVE-2003-1025 CVE-2003-1026 CVE-2003-1027 CVE-2003-1326 CVE-2003-1328	no
win2k	potential	Javaprxy.dll access through Internet Explorer	Windows OS	CVE-2005-2087	yes
win2k	potential	last user name shown in login box	Windows OS	CVE-1999-0592	no

win2k	potential	Possible vulnerability in LDAP over SSL	Other	CVE-2001-0502	no
win2k	potential	Is your LDAP secure?	Other	CVE-2002-1378 CVE-2002-1379	no
win2k	potential	Authentication flaw in Microsoft mail server	Mail	CVE-2001-0504 CVE-2002-0054	no
win2k	potential	Possible vulnerability in MS SQL Server Resolution Service	Databases	CVE-2002-0649 CVE-2002-0650 CVE-2002-0729	yes
win2k	potential	Possible vulnerability in Microsoft Terminal Server	Other	CVE-2000-1149 CVE-2001-0663 CVE-2001-0716 CVE-2002-0863 CVE-2002-0864 CVE-2005-1218	no
win2k	potential	The NT Alerter and Messenger services are running	Other	CVE-1999-0630	no
win2k	potential	NetBIOS share enumeration using null session	Windows OS		no
win2k	potential	Windows null session domain SID disclosure	Windows OS	CVE-2000-1200	no
win2k	potential	Windows null session host SID disclosure	Windows OS		no
win2k	potential	excessive null session access	Windows OS	CVE-2000-1200	no
win2k	potential	Obsolete Windows Release: Windows 2000	Other		no
win2k	potential	Outlook Express MHTML vulnerability	Mail	CVE-2004-0380	no
win2k	potential	Outlook Express NNTP buffer overflow	Mail	CVE-2005-1213	yes
win2k	potential	Outlook Express patch needed	Mail	CVE-2002-1179	no
win2k	potential	chargen could be used in UDP bomb	Networking /SNMP	CVE-1999-0103 CVE-1999-0639	no
win2k	potential	SMTP may be a mail relay	Mail	CVE-1999-0512	no
win2k	potential	SNMP is enabled and may be vulnerable	Networking /SNMP	CVE-2002-0012 CVE-2002-0013 CVE-2002-0053	no
win2k	potential	User TsInternetUser has never logged in	Windows OS		no
win2k	potential	Web server default page detected	Web		no
win2k	potential	password complexity policy disabled	Windows OS	CVE-1999-0535	no
win2k	potential	weak account lockout policy (0)	Windows OS	CVE-1999-0582	no
win2k	potential	weak minimum password age policy (0 days)	Windows OS	CVE-1999-0535	no
win2k	potential	weak minimum password length policy (0)	Windows OS	CVE-1999-0535	no
win2k	potential	weak password history policy (1)	Windows OS	CVE-1999-0535	no
win2k	potential	non-administrative users can act as part of the operating system	Windows OS	CVE-1999-0534	no
win2k	potential	non-administrative users can bypass traverse checking	Windows OS	CVE-1999-0534	no
win2k	potential	non-administrative users can replace a process level token	Windows OS	CVE-1999-0534	no
win2k	potential	auditing is disabled	Windows OS	CVE-1999-0575	no
win2k	potential	Windows administrator account not renamed	Windows OS	CVE-1999-0585	no
win2k	potential	Windows guest account not renamed	Windows OS		no
win2k	potential	Password never expires for user IUSR_SAINTLAB02	Windows OS		no
win2k	potential	Password never expires for user IWAM_SAINTLAB02	Windows OS		no
win2k	potential	Password never expires for user NetShowServices	Windows OS		no
win2k	potential	Password never expires for user TsInternetUser	Windows OS		no
win2k	potential	Password never expires for user kline	Windows OS		no

win2k	potential	Password never expires for user testadmin	Windows OS		no
win2k	potential	Collaboration Data Objects vulnerability	Windows OS	CVE-2005-1987	no
win2k	potential	FTP Client vulnerability	Windows OS	CVE-2005-2126	no
win2k	potential	HTML Help ActiveX Control remote code execution	Windows OS	CVE-2007-0214	no
win2k	potential	HTML Help ActiveX Control string buffer overflow	Windows OS	CVE-2006-3357	no
win2k	potential	Jet Database Engine buffer overflow	Windows OS	CVE-2004-0197	no
win2k	potential	Jet Database Engine input validation problems	Windows OS	CVE-2005-0944	yes
win2k	potential	Microsoft Agent spoofing vulnerability	Windows OS	CVE-2005-1214	no
win2k	potential	Multiple Windows TCP/IP vulnerabilities (MS08-001)	Windows OS	CVE-2007-0066 CVE-2007-0069	no
win2k	potential	Network Connection Manager vulnerability	Windows OS	CVE-2005-2307	no
win2k	potential	Win2000 Multiple UNC Provider buffer overflow	Windows OS	CVE-1999-0662 CVE-2002-0151	no
win2k	potential	Win2000 SP2 Security Rollup 1 not installed	Windows OS	CVE-1999-0662	no
win2k	potential	Win2000 unchecked buffer in Remote Access Service Phonebook	Windows OS	CVE-1999-0662 CVE-2002-0366	no
win2k	potential	Windows 2000 HTML Converter buffer overflow	Windows OS	CVE-2003-0469	no
win2k	potential	Windows 2000 NetMeeting directory traversal	Windows OS	CVE-2003-0505 CVE-2003-0506	no
win2k	potential	Windows 2000 Network Connection Manager flaw	Windows OS	CVE-1999-0662 CVE-2002-0720	no
win2k	potential	Windows 2000 RPC denial of service	Windows OS	CVE-1999-0662 CVE-2001-0509	no
win2k	potential	Windows 2000 SP4 Update Rollup 1 not applied	Windows OS	CVE-2005-3168 CVE-2005-3169 CVE-2005-3170 CVE-2005-3171 CVE-2005-3172 CVE-2005-3173 CVE-2005-3174 CVE-2005-3175 CVE-2005-3176 CVE-2005-3177	no
win2k	potential	Windows 2000 ShellExecute API buffer overflow	Windows OS	CVE-2003-0503	no
win2k	potential	Windows 2000 VM ByteCode Verifier vulnerability	Windows OS	CVE-2003-0111	no
win2k	potential	Windows 2000 VM COM object access	Windows OS	CVE-1999-0662 CVE-2002-1257 CVE-2002-1258 CVE-2002-1260 CVE-2002-1262 CVE-2002-1286 CVE-2002-1292 CVE-2002-1295	no
win2k	potential	Windows 2000 VM JDBC Classes vulnerability	Windows OS	CVE-1999-0662 CVE-2002-0865 CVE-2002-0866 CVE-2002-0867	no
win2k	potential	Windows 2000 browser applet redirect	Windows OS	CVE-1999-0662 CVE-2002-0058 CVE-2002-0076	no
win2k	potential	Windows 2000 certificate validation flaw	Windows OS	CVE-1999-0662 CVE-2002-0862	no

win2k	potential	Windows 2000 debugger authentication flaw	Windows OS	CVE-1999-0662 CVE-2002-0367	no
win2k	potential	Windows 2000 help facility buffer overflow	Windows OS	CVE-1999-0662 CVE-2002-0693 CVE-2002-0694	no
win2k	potential	Windows 2000 ntdll.dll buffer overflow	Windows OS	CVE-2003-0109	yes
win2k	potential	Windows 2000 relative shell path	Windows OS	CVE-1999-0662 CVE-2000-0663	no
win2k	potential	Windows 2000 shell buffer overflow	Windows OS	CVE-1999-0662 CVE-2002-0070	no
win2k	potential	Windows 2000 unchecked buffer in network share provider can lead to DoS	Windows OS	CVE-1999-0662 CVE-2002-0724	no
win2k	potential	Windows HTML Help input validation vulnerability	Windows OS	CVE-2003-1041 CVE-2004-0201	no
win2k	potential	Windows HyperTerminal buffer overflow	Windows OS	CVE-2004-0568	no
win2k	potential	Windows Media Player URL script execution	Windows OS	CVE-2003-1107	no
win2k	potential	Windows Message Queuing vulnerability	Windows OS	CVE-2005-0059	yes
win2k	potential	Windows RPC mutual authentication spoofing	Windows OS	CVE-2006-2380	no
win2k	potential	Windows Shell API CLSID vulnerability	Windows OS	CVE-2004-0420	no
win2k	potential	Windows Task Scheduler buffer overflow	Windows OS	CVE-2004-0212	yes
win2k	potential	Windows authenticode verification vulnerability	Windows OS	CVE-2003-0660	no
win2k	potential	Windows help and support center buffer overflow	Windows OS	CVE-2003-0711	no
win2k	potential	Windows troubleshooter ActiveX control vulnerability	Windows OS	CVE-2003-0662	no
win2k	potential	Wordpad Word-for-Windows Converter buffer overflow	Windows OS	CVE-2004-0571 CVE-2004-0901	no
win2k	potential	possible Microsoft DirectX buffer overflow	Windows OS	CVE-2003-0346	no
win2k	potential	potential vulnerability in WINS	Windows OS	CVE-2003-0825	no
win2k	service	17/TCP			no
win2k	service	17/UDP			no
win2k	service	42/TCP			no
win2k	service	88/TCP			no
win2k	service	88/UDP			no
win2k	service	464/TCP			no
win2k	service	464/UDP			no
win2k	service	548/TCP			no
win2k	service	563/TCP			no
win2k	service	593/TCP			no
win2k	service	1026/TCP			no
win2k	service	1028/UDP			no
win2k	service	1029/TCP			no
win2k	service	1051/TCP			no
win2k	service	1052/UDP			no
win2k	service	1054/UDP			no
win2k	service	1057/TCP			no
win2k	service	1061/UDP			no
win2k	service	1066/UDP			no
win2k	service	1069/UDP			no
win2k	service	1079/UDP			no
win2k	service	1086/TCP			no
win2k	service	1089/TCP			no
win2k	service	1103/UDP			no

win2k	service	1104/UDP	no
win2k	service	1106/TCP	no
win2k	service	1107/TCP	no
win2k	service	1108/TCP	no
win2k	service	1109/UDP	no
win2k	service	1111/TCP	no
win2k	service	1112/UDP	no
win2k	service	1113/TCP	no
win2k	service	1117/UDP	no
win2k	service	1127/UDP	no
win2k	service	1135/TCP	no
win2k	service	1138/UDP	no
win2k	service	1144/TCP	no
win2k	service	1152/UDP	no
win2k	service	1243/UDP	no
win2k	service	1350/UDP	no
win2k	service	1383/UDP	no
win2k	service	1433/TCP	no
win2k	service	1434/UDP	no
win2k	service	1645/UDP	no
win2k	service	1646/UDP	no
win2k	service	1718/UDP	no
win2k	service	1719/UDP	no
win2k	service	1755/TCP	no
win2k	service	1755/UDP	no
win2k	service	1801/TCP	no
win2k	service	1801/UDP	no
win2k	service	1813/UDP	no
win2k	service	2101/TCP	no
win2k	service	2103/TCP	no
win2k	service	2107/TCP	no
win2k	service	3268/TCP	no
win2k	service	3269/TCP	no
win2k	service	3372/TCP	no
win2k	service	3389/TCP	no
win2k	service	6666/TCP	no
win2k	service	7007/TCP	no
win2k	service	7778/TCP	no
win2k	service	DNS	no
win2k	service	FTP	no
win2k	service	FTP (with anonymous)	no
win2k	service	NNTP (Usenet news)	no
win2k	service	SMB	no
win2k	service	SMTP	no
win2k	service	SNMP	no
win2k	service	WWW	no
win2k	service	WWW (Secure)	no
win2k	service	WWW (non-standard port 5406)	no
win2k	service	XDM (X login)	no
win2k	service	bootpc (68/UDP)	no
win2k	service	bootps (67/UDP)	no
win2k	service	chargen (19/TCP)	no
win2k	service	chargen:UDP (19/UDP)	no
win2k	service	daytime (13/TCP)	no

win2k	service	daytime (13/UDP)	no
win2k	service	discard (9/TCP)	no
win2k	service	discard (9/UDP)	no
win2k	service	domain (53/UDP)	no
win2k	service	echo (7/TCP)	no
win2k	service	echo (7/UDP)	no
win2k	service	eklogin (2105/TCP)	no
win2k	service	epmap (135/TCP)	no
win2k	service	epmap (135/UDP)	no
win2k	service	isakmp (500/UDP)	no
win2k	service	ldap (389/TCP)	no
win2k	service	ldap (389/UDP)	no
win2k	service	microsoft-ds (445/TCP)	no
win2k	service	microsoft-ds (445/UDP)	no
win2k	service	name (42/UDP)	no
win2k	service	netbios-dgm (138/UDP)	no
win2k	service	netbios-ns (137/UDP)	no
win2k	service	ntp (123/UDP)	no
win2k	service	printer (515/TCP)	no
win2k	service	radius (1812/UDP)	no
win2k	service	ssl-ldap (636/TCP)	no
win2k	service	tftp (69/UDP)	no
win2k	info	Netbios Attribute: Domain Controller	no
win2k	info	Netbios Attribute: Master Browser	no
win2k	info	Netbios Attribute: Messenger Service	no
win2k	info	Netbios Attribute: Primary Domain Controller	no
win2k	info	Share: ADMIN$	no
win2k	info	Share: C$	no
win2k	info	Share: E$	no
win2k	info	Share: NETLOGON	no
win2k	info	Share: SYSVOL	no
win2k	info	User: Administrator (500)	no
win2k	info	User: DHCP Administrators (1006)	no
win2k	info	User: DHCP Users (1005)	no
win2k	info	User: DnsAdmins (1108)	no
win2k	info	User: DnsUpdateProxy (1109)	no
win2k	info	User: Guest (501) (disabled)	no
win2k	info	User: IUSR_SAINTLAB02 (1003)	no
win2k	info	User: IWAM_SAINTLAB02 (1004)	no
win2k	info	User: NetShow Administrators (1002)	no
win2k	info	User: NetShowServices (1001)	no
win2k	info	User: SAINTLAB02$ (1007)	no
win2k	info	User: SAINTLAB3W2K$ (1113)	no
win2k	info	User: SAINTLAB3W2K3$ (1117)	no
win2k	info	User: SAINTLAB4W2K3SW$ (1116)	no
win2k	info	User: SAINTLABXP$ (1112)	no
win2k	info	User: TsInternetUser (1000)	no
win2k	info	User: WINS Users (1110)	no
win2k	info	User: kline (1121)	no
win2k	info	User: testadmin (1111)	no
win2k	info	Windows service: Alerter	no
win2k	info	Windows service: COM+ Event System	no
win2k	info	Windows service: Computer Browser	no

win2k	info	Windows service: DHCP Client	no
win2k	info	Windows service: DHCP Server	no
win2k	info	Windows service: DNS Client	no
win2k	info	Windows service: DNS Server	no
win2k	info	Windows service: Distributed File System	no
win2k	info	Windows service: Distributed Link Tracking Client	no
win2k	info	Windows service: Distributed Link Tracking Server	no
win2k	info	Windows service: Distributed Transaction Coordinator	no
win2k	info	Windows service: Event Log	no
win2k	info	Windows service: FTP Publishing Service	no
win2k	info	Windows service: File Replication Service	no
win2k	info	Windows service: File Server for Macintosh	no
win2k	info	Windows service: IIS Admin Service	no
win2k	info	Windows service: IPSEC Policy Agent	no
win2k	info	Windows service: Internet Authentication Service	no
win2k	info	Windows service: Intersite Messaging	no
win2k	info	Windows service: Kerberos Key Distribution Center	no
win2k	info	Windows service: License Logging Service	no
win2k	info	Windows service: Logical Disk Manager	no
win2k	info	Windows service: MSSQLSERVER	no
win2k	info	Windows service: Message Queuing	no
win2k	info	Windows service: Messenger	no
win2k	info	Windows service: Microsoft Search	no
win2k	info	Windows service: NT LM Security Support Provider	no
win2k	info	Windows service: Net Logon	no
win2k	info	Windows service: Network News Transport Protocol (NNTP)	no
win2k	info	Windows service: Plug and Play	no
win2k	info	Windows service: Print Server for Macintosh	no
win2k	info	Windows service: Print Spooler	no
win2k	info	Windows service: Protected Storage	no
win2k	info	Windows service: Remote Procedure Call (RPC)	no
win2k	info	Windows service: Remote Procedure Call (RPC) Locator	no
win2k	info	Windows service: Remote Registry Service	no
win2k	info	Windows service: Removable Storage	no
win2k	info	Windows service: RunAs Service	no
win2k	info	Windows service: SNMP Service	no
win2k	info	Windows service: Security Accounts Manager	no
win2k	info	Windows service: Server	no
win2k	info	Windows service: Simple Mail Transport Protocol (SMTP)	no
win2k	info	Windows service: Simple TCP/IP Services	no
win2k	info	Windows service: System Event Notification	no
win2k	info	Windows service: TCP/IP NetBIOS Helper Service	no
win2k	info	Windows service: TCP/IP Print Server	no

win2k	info	Windows service: Task Scheduler	no
win2k	info	Windows service: Telephony	no
win2k	info	Windows service: Terminal Services	no
win2k	info	Windows service: Terminal Services Licensing	no
win2k	info	Windows service: Windows Internet Name Service (WINS)	no
win2k	info	Windows service: Windows Management Instrumentation	no
win2k	info	Windows service: Windows Management Instrumentation Driver Extensions	no
win2k	info	Windows service: Windows Media Monitor Service	no
win2k	info	Windows service: Windows Media Program Service	no
win2k	info	Windows service: Windows Media Station Service	no
win2k	info	Windows service: Windows Media Unicast Service	no
win2k	info	Windows service: Windows Time	no
win2k	info	Windows service: Workstation	no
win2k	info	Windows service: World Wide Web Publishing Service	no

5.0 Details

The following sections provide details on the specific vulnerabilities detected on each host.

5.1 win2k

IP Address: 10.7.0.2
Scan time: Feb 03 09:07:07 2012
Host type: Windows 2000 SP2
Netbios Name: SAINTLAB02

Active Directory LDAP request memory allocation vulnerability

Severity: Critical Problem **CVE:** CVE-2008-4023

Impact

A remote attacker could crash the Active Directory service and force a reboot of the server. It may also be possible to execute commands on the server.

Resolution

Install the patches referenced in Microsoft Security Bulletin 09-066.

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-039, 08-003, 08-035, 08-060, 09-018, and 09-066.

Technical Details

Service: registry
LDAP or LDAPS running and KB957280 not applied