Remediation Plan

1. Discovered Systems

Node	Operating System	Risk	Aliases
10.2.53.211	Microsoft Windows XP Professional SP2	17.31	•iml-desktop2
10.2.51.250	Ubuntu Linux	9.11	•iml-accounting

2. Risk Assessment

This report identifies security risks that could adversely affect your critical operations and assets. These risks are quantified according to their likelihood of occurrence and the potential damage if they occur. Risk factors are combined to form an overall risk index for each system, allowing you to prioritize your remediation activities accordingly.

Device	Risk Index	Risk Factors
10.2.53.211 (iml-desktop2)	17.31	•This device is in the Boston - LAN site with a risk factor of 1.00. •68 critical vulnerabilities were discovered with a risk weight of 12.24. •52 severe vulnerabilities were discovered with a risk weight of 5.72. •5 moderate vulnerabilities were discovered with a risk weight of 0.20. •2 CIFS services were discovered with a risk weight of 0.10. •One NTP service was discovered with a risk weight of 0.05. •One CIFS Name Service service was discovered with a risk weight of 0.05. •One DCE Endpoint Resolution service was discovered with a risk weight of 0.05.
10.2.51.250 (iml-accounting)	9.11	•This device is in the Boston - Production site with a risk factor of 1.00. •22 critical vulnerabilities were discovered with a risk weight of 3.96. •19 severe vulnerabilities were discovered with a risk weight of 2.09. •One Oracle service was discovered with a risk weight of 3.00. •One SSH service was discovered with a risk weight of 0.05. •One HTTP service was discovered with a risk weight of 0.05. •One FTPS service was discovered with a risk weight of 0.05.

3. Remediation Plan

3.1. Remediation Plan for 10.2.53.211 (iml-desktop2)

3.1.1. For Microsoft Windows XP Professional SP2

These vulnerabilities can be resolved by performing the following 41 steps. The total estimated time to perform all of these steps is 19 hours 20 minutes.

Download and install Microsoft patch WindowsXP-KB936929-SP3-x86-ENU.exe (316.4 MB)

Estimated time: 20 minutes

Microsoft Windows XP Professional < SP3, Microsoft Winodws XP Home < SP3

Download and apply the upgrade from: http://download.microsoft.com/download/d/3/0/d30e32d8-418a-469d-b600-f32ce3edf42d/WindowsXP-KB936929-SP3-x86-ENU.exe

This will address the following 29 issues:

•Windows XP Service Pack 3 (KB936929) (servicepack-windows-xp-sp3)

•MS07-006: Vulnerability in Windows Shell Could Allow Elevation of Privilege (928255) (WINDOWS-HOTFIX-MS07-006)

•MS07-007: Vulnerability in Windows Image Acquisition Service Could Allow Elevation of Privilege (927802) (WINDOWS-HOTFIX-MS07-007)

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

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

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

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

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

•MS07-017: Vulnerability In GDI Could Allow Remote Code Execution (925902) (WINDOWS-HOTFIX-MS07-017)

•MS07-019: Vulnerability in Universal Plug and Play Could Allow Remote Code Execution (931261) (WINDOWS-HOTFIX-MS07-019)

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

•MS07-021: Vulnerability in CSRSS Could Allow Remote Code Execution (930178) (WINDOWS-HOTFIX-MS07-021)

•MS07-022: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784) (WINDOWS-HOTFIX-MS07-022)

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

•MS07-034: Cumulative Security Update for Outlook Express and Windows Mail (929123) (WINDOWS-HOTFIX-MS07-034)

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

•MS07-043: Vulnerability in OLE Automation Could Allow Remote Code Execution (921503) (WINDOWS-HOTFIX-MS07-043)

•MS07-046: Vulnerability in GDI Could Allow Remote Code Execution (938829) (WINDOWS-HOTFIX-MS07-046)

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

•MS07-058: Vulnerability in RPC Could Allow Denial of Service (933729) (WINDOWS-HOTFIX-MS07-058)

•MS07-065: Vulnerability in Message Queuing Could Allow Remote Code Execution (937894) (WINDOWS-HOTFIX-MS07-065)

•MS07-068: Vulnerability in Windows Media File Format Could Allow Remote Code Execution (941569 and 944275) (WINDOWS-HOTFIX-MS07-068)
•MS08-002: Vulnerability in LSASS Could Allow Local Elevation of Privilege (943485) (WINDOWS-HOTFIX-MS08-002)
•MS08-007: Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026) (WINDOWS-HOTFIX-MS08-007)
•MS08-008: Vulnerability in OLE Automation Could Allow Remote Code Execution (947890) (WINDOWS-HOTFIX-MS08-008)
•MS08-020: Vulnerability in DNS Client Could Allow Spoofing (945553) (WINDOWS-HOTFIX-MS08-020)
•MS08-021: Vulnerabilities in GDI Could Allow Remote Code Execution (948590) (WINDOWS-HOTFIX-MS08-021)
•MS08-025: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693) (WINDOWS-HOTFIX-MS08-025)
•MS08-028: Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution (950749) (WINDOWS-HOTFIX-MS08-028)

Download and install Microsoft patch WindowsXP-KB958687-x86-ENU.exe (658288 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2008/12/windowsxp-kb958687-x86-enu_a9b85264e9b75e552ae10cd212937b8686a96833.exe
This will address the following 4 issues:
•MS08-063: Vulnerability in SMB Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS08-063)
•3 instances of MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-001)

Download and install Microsoft patch WindowsXP-KB969947-x86-ENU.exe (1474928 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/10/windowsxp-kb969947-x86-enu_12b63bf594ba6547a6bc94acecd4572a75e3eb44.exe
This will address the following 3 issues:
•MS08-061: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (WINDOWS-HOTFIX-MS08-061)
•MS09-006: Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-006)
•MS09-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (WINDOWS-HOTFIX-MS09-025)

Download and install Microsoft patch WindowsXP-KB971633-x86-ENU.exe (1044856 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/06/windowsxp-kb971633-x86-enu_53c185a01195b208ebbefa903f703dc668698bbb.exe
This will address the following 3 issues:
•MS08-033: Vulnerabilities in DirectX Could Allow Remote Code Execution (951698) (WINDOWS-HOTFIX-MS08-033)
•MS09-011: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-011)
•MS09-028: Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-028)

Set the password expiration

Estimated time: 30 minutes

Microsoft Windows 2000 Professional, Microsoft Windows XP Professional
If the account is not used, delete or disable the account. If the account is a built-in system account such as the IUSR_ or IWAM_ accounts, enable the "User cannot change password" option to stop this vulnerability from being reported (Microsoft best practices dictate that built-in system accounts NOT be allowed to change their own passwords). Otherwise, ensure that the password expires by disabling the "Password never expires" option.

1. Right click on "My Computer"
2. Select "Manage"
3. Open the "Local Users and Groups" folder
4. Open the "Users" folder
5. Double-click on the desired user
6. Uncheck "Password never expires"

This will address 2 instances of the following issue: CIFS Account Password Never Expires (cifs-acct-password-never-expires).

Download and install Microsoft patch WindowsXP-KB973525-x86-ENU.exe (498552 bytes)
Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/09/windowsxp-kb973525-x86-enu_81227dc379d43ad8ac33daaffe7576ee1a942c2e.exe
This will address the following 2 issues:
•MS08-032: Cumulative Security Update of ActiveX Kill Bits (950760) (WINDOWS-HOTFIX-MS08-032)
•MS09-032: Cumulative Security Update of ActiveX Kill Bits (WINDOWS-HOTFIX-MS09-032)

Download and install Microsoft patch WindowsXP-KB956572-x86-ENU.exe (4574080 bytes)
Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/03/windowsxp-kb956572-x86-enu_a2463f484318332e8319dd931c87b27cf747b2de.exe
This will address the following 2 issues:
•MS08-064: Vulnerability in Virtual Address Descriptor Manipulation Could Allow Elevation of Privilege (WINDOWS-HOTFIX-MS08-064)
•MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege (WINDOWS-HOTFIX-MS09-012)

Download and install Microsoft patch WindowsXP-KB958644-x86-ENU.exe (648560 bytes)
Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2008/10/windowsxp-kb958644-x86-enu_5c135a8dae5721849430afe27af255f83e64f62b.exe
This will address the following issue: MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS08-067).

Download and install Microsoft patch WindowsXP-KB960859-x86-ENU.exe (559472 bytes)
Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/07/windowsxp-kb960859-x86-enu_c1a1e20576bc745a720053357e46be6c2a3f7faa.exe
This will address the following issue: MS09-042: Vulnerability in Telnet Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-042).

Download and install Microsoft patch WindowsXP-KB956844-x86-ENU.exe (563576 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/07/windowsxp-kb956844-x86-enu_926002701569eabda17630d8f9cb45d8ced0ab71.exe
This will address the following issue: MS09-046: Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-046).

Download and install Microsoft patch WindowsXP-KB943460-x86-ENU.exe

Estimated time: 15 minutes
Microsoft Windows XP Professional SP2 (x86), Microsoft Windows XP Home SP2 (x86)
Download and apply the patch from: http://download.microsoft.com/download/0/e/b/0eb29ece-fb34-4eb6-ae49-a6e816a9fa5b/WindowsXP-KB943460-x86-ENU.exe
This will address the following issue: MS07-061: Vulnerability in Windows URI Handling Could Allow Remote Code Execution (943460) (WINDOWS-HOTFIX-MS07-061).

Download and install Microsoft patch WindowsXP-KB971557-x86-ENU.exe (535416 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/07/windowsxp-kb971557-x86-enu_8364a52ae5693fb52221ffce5cc943c35013de32.exe
This will address the following issue: MS09-038: Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-038).

Download and install Microsoft patch WindowsXP-SP2-WindowsMedia-KB968816-x86-ENU.exe (4863368 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP2 (x86), Microsoft Windows XP Home SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/08/windowsxp-sp2-windowsmedia-kb968816-x86-enu_3398453408452312e1cf2bf93a082f979803db0a.exe
This will address the following issue: MS09-047: Vulnerabilities in Windows Media Format Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-047).

Download and install Microsoft patch WindowsXP-KB973354-x86-ENU.exe (1064816 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/07/windowsxp-kb973354-x86-enu_bdd4b9aa97255fc5b7300ddafbe306139e3005ba.exe
This will address the following issue: MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-037).

Download and install Microsoft patch WindowsXP-KB951376-v2-x86-ENU.exe (605224 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/software/secu/2008/06/windowsxp-kb951376-v2-x86-enu_e9b68c5e63acb5786a05b53b4332465de0ebcebd.exe
This will address the following issue: MS08-030: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (951376) (WINDOWS-HOTFIX-MS08-030).

Download and install Microsoft patch WindowsXP-kb971961-JS57-X86-ENU.exe (725360 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/08/windowsxp-kb971961-js57-x86-enu_9722544230b316cbd21740ed56dc7a9e7af9603b.exe
This will address the following issue: MS09-045: Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-045).

Download and install Microsoft patch WindowsXP-KB944338-v2-x86-ENU.exe (826920 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP2 (x86), Microsoft Windows XP Home SP2 (x86)
Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/software/secu/2008/07/windowsxp-kb944338-v2-x86-enu_d8cade8456591867f22cdae4c42db7f473afbd67.exe
This will address the following issue: MS08-022: Vulnerability in VBScript and JScript Scripting Engines Could Allow Remote Code Execution (944338) (WINDOWS-HOTFIX-MS08-022).

Download and install Microsoft patch WindowsXP-KB961501-x86-ENU.exe (662896 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/05/windowsxp-kb961501-x86-enu_a5360324a1fe219a9aa9f0e513edffe7305176e4.exe
This will address the following issue: MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-022).

Download and install Microsoft patch WindowsXP-KB971657-x86-ENU.exe (561528 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/07/windowsxp-kb971657-x86-enu_697f5d861910aa051131a58e1af607a79e14e1a9.exe
This will address the following issue: MS09-041: Vulnerability in Workstation Service Could Allow Elevation of Privilege (WINDOWS-HOTFIX-MS09-041).

Download and install Microsoft patch WindowsXP-KB957097-x86-ENU.exe (725360 bytes)

Estimated time: 30 minutes
Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2008/11/windowsxp-kb957097-x86-enu_af78065a797e9fb4c03ba811b04db6a66fa6e2d0.exe
This will address the following issue: MS08-068: Vulnerability in SMB Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS08-068).

Download and install Microsoft patch WindowsXP-SP2-WindowsMedia-KB952069-v2-x86-ENU.exe (8822672 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP2 (x86), Microsoft Windows XP Home SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/01/windowsxp-sp2-windowsmedia-kb952069-v2-x86-enu_97de22fb2fed50fb03e1107b579975f2295feb8a.exe

This will address the following issue: MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS08-076).

Download and install Microsoft patch WindowsXP-KB970238-x86-ENU.exe (878464 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/05/windowsxp-kb970238-x86-enu_82bd58dd365d93afa746a4beaf2a1ad5b8d5181a.exe

This will address the following issue: MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (WINDOWS-HOTFIX-MS09-026).

Download and install Microsoft patch WindowsXP-KB960225-x86-ENU.exe (569712 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/01/windowsxp-kb960225-x86-enu_bae2bc04b963c312a47f36bdea4a8236f7003d71.exe

This will address the following issue: MS09-007: Vulnerability in SChannel Could Allow Spoofing (WINDOWS-HOTFIX-MS09-007).

Download and install Microsoft patch WindowsXP-KB951066-x86-ENU.exe (817704 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/software/secu/2008/05/windowsxp-kb951066-x86-enu_a797af170113a4be4f87b7c1eb1173f0c28a58ee.exe

This will address the following issue: MS07-056: Security Update for Outlook Express and Windows Mail (941202) (WINDOWS-HOTFIX-MS07-056).

Download and install Microsoft patch WindowsXP-KB956802-x86-ENU.exe (639856 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2008/11/windowsxp-kb956802-x86-enu_bf0a8bfe0d01487a999fb8f66b3719957acf1f3a.exe

This will address the following issue: MS08-071: Vulnerabilities in GDI Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS08-071).

Download and install Microsoft patch WindowsXP-KB960803-x86-ENU.exe (671088 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/03/windowsxp-kb960803-x86-enu_114aa39cb3e1e42c0f9897c99e697084dbdc656f.exe

This will address the following issue: MS09-013: Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-013).

Download and install Microsoft patch WindowsXP-KB959426-x86-ENU.exe (845712 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/03/windowsxp-kb959426-x86-enu_9bdfabdec1c98057a92503cb00ce6ed623b517c5.exe

This will address the following issue: MS09-015: Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (WINDOWS-HOTFIX-MS09-015).

Download and install Microsoft patch WindowsXP-KB923561-x86-ENU.exe (1264016 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/04/windowsxp-kb923561-x86-enu_b8aac16b07ca89c7dde4d724c808ff88faa456ec.exe

This will address the following issue: MS09-010: Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-010).

Download and install Microsoft patch WindowsXP-KB961371-v2-x86-ENU.exe (568688 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/08/windowsxp-kb961371-v2-x86-enu_ef9b80c7dfe521243e130fbc441646498a0da5c2.exe

This will address the following issue: MS09-029: Vulnerabilities in the Embedded OpenType Font Engine Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS09-029).

Download and install Microsoft patch WindowsXP-KB971032-x86-ENU.exe (1391992 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP2 (x86), Microsoft Windows XP Home SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/07/windowsxp-kb971032-x86-enu_23f7ac835ed26257c74a7b1ef5caa6198182cf6c.exe

This will address the following issue: MS09-040: Vulnerability in Message Queuing Could Allow Elevation of Privilege (WINDOWS-HOTFIX-MS09-040).

Download and install Microsoft patch WindowsXP-KB956803-x86-ENU.exe (570408 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2008/09/windowsxp-kb956803-x86-enu_d075d359a28ab8b058a35a2e7b466bd0bca8e9ef.exe

This will address the following issue: MS08-066: Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege (WINDOWS-HOTFIX-MS08-066).

Download and install Microsoft patch WindowsXP-KB955069-x86-ENU.exe (926760 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2008/09/windowsxp-kb955069-x86-enu_fa864585a7d761ba0f940eff151672871d0e69f3.exe

This will address the following issue: MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (WINDOWS-HOTFIX-MS08-069).

Set an account lockout threshold

Estimated time: 15 minutes

Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

1. Open the "Performance and Maintenance" control panel.
2. Select "Administrative Tools".
3. To change the domain-wide lockout policy, select "Domain Security Policy" (or "Domain Controller Security Policy" if the computer is a Domain Controller). Otherwise, to change the policy for this computer only, select "Local Security Policy."
4. Expand the "Account Policies" folder and select "Account Lockout Policy".
5. Set the Account Lockout Duration. This setting controls the amount of time an account will remain locked after repeated failed login attempts. To keep accounts locked until the Administrator intervenes, set the lockout duration to 0. Otherwise, be sure to use a reasonable value, preferably 1440 minutes (1 day) or greater.
6. Set the Account Lockout Threshold. This setting determines the number of successive failed login attempts that will cause the account to be locked. Set the lockout threshold to 3 or fewer.
7. Restart the system for the changes to take effect.

This will address the following issue: CIFS Account Lockout Policy Not Enforced (cifs-no-acct-lockout-limit).

Download and install Microsoft patch WindowsXP-KB950762-x86-ENU.exe (559144 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/software/secu/2008/05/windowsxp-kb950762-x86-enu_bfa04c9d2e62b4695d1bb8953486788c8a8c11e4.exe

This will address the following issue: MS08-036: Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service (950762) (WINDOWS-HOTFIX-MS08-036).

Download and install Microsoft patch WindowsXP-SP2-WindowsMedia-KB973540-x86-ENU.exe (9847176 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP2 (x86), Microsoft Windows XP Home SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/07/windowsxp-sp2-windowsmedia-kb973540-x86-enu_dff9fd1cafd1b740784f00e43a3aff588d0c810d.exe

This will address the following issue: MS07-047: Vulnerabilities in Windows Media Player Could Allow Remote Code Execution (936782) (WINDOWS-HOTFIX-MS07-047).

Download and install Microsoft patch WindowsXP-KB950974-x86-ENU.exe (594984 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/software/secu/2008/07/windowsxp-kb950974-x86-enu_fd840632e13df756e9d1251400e6e659d16a8b27.exe

This will address the following issue: MS08-049: Vulnerabilities in Event System Could Allow Remote Code Execution (950974) (WINDOWS-HOTFIX-MS08-049).

Download and install Microsoft patch WindowsXP-KB969898-x86-ENU.exe (497528 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the upgrade from: http://download.windowsupdate.com/msdownload/update/software/uprl/2009/05/windowsxp-kb969898-x86-enu_907eead29c7f8ba8fcc11ade8245663aa2d84c3e.exe

This will address the following issue: Update Rollup for ActiveX Killbits for Windows XP (KB969898) (updaterollup-activex-killbits-winxp-x86).

Set the minimum password length

Estimated time: 15 minutes

Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

1. Open the "Performance and Maintenance" control panel.
2. Select "Administrative Tools".
3. To change the domain-wide lockout policy, select "Domain Security Policy" (or "Domain Controller Security Policy" if the computer is a Domain Controller). Otherwise, to change the policy for this computer only, select "Local Security Policy."
4. Expand the "Account Policies" folder and select "Password Policy".
5. Set the Minimum Password Length. This setting enforces a minimum length for new or changed passwords. A value of 6 or higher is recommended.
6. Note that this policy does not affect existing passwords. It will only take effect when an existing user changes his password.

This will address the following issue: CIFS Minimum Password Length Policy Not Enforced (cifs-no-password-length-min).

Download and install Microsoft patch WindowsXP-KB951066-x86-ENU.exe (817704 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/software/secu/2008/05/windowsxp-kb951066-x86-enu_a797af170113a4be4f87b7c1eb1173f0c28a58ee.exe

This will address the following issue: MS08-048: Security Update for Outlook Express and Windows Mail (951066) (WINDOWS-HOTFIX-MS08-048).

Download and install Microsoft patch WindowsXP-KB946648-x86-ENU.exe (528424 bytes)

Estimated time: 30 minutes

Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/software/secu/2008/05/windowsxp-kb946648-x86-enu_288da0ecf75b20e972ad58dba0a382173b548ec1.exe

This will address the following issue: MS08-050: Vulnerability in Windows Messenger Could Allow Information Disclosure (955702) (WINDOWS-HOTFIX-MS08-050).

Disable NULL sessions

Estimated time: 15 minutes

Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional

Modify the registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
with the following values:

```
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Data Value: 1

Value Name: RestrictAnonymousSAM
Data Type: REG_DWORD
Data Value: 1

Value Name: EveryoneIncludesAnonymous
Data Type: REG_DWORD
Data Value: 0
```

Modify the registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\
with the following values:

```
Value Name: RestrictNullSessAccess
Data Type: REG_DWORD
Data Value: 1

Value Name: NullSessionPipes
Data Type: REG_MULTI_SZ
Data Value: "" (empty string, without quotes)
```

Open Local Security Settings, and disable the following setting:

```
Security Settings -> Local Policies -> Security Options ->
Network access: Allow anonymous SID/Name translation: Disabled
```

Finally, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to Microsoft Knowledge Base Article Q246261 for more information.

This will address the following issue: CIFS NULL Session Permitted (CIFS-NT-0001).

3.1.2. General

These vulnerabilities can be resolved by performing the following 13 steps. The total estimated time to perform all of these steps is 8 hours 25 minutes.

Install the newest version of Mozilla

Estimated time: 30 minutes

Install the latest version of Mozilla Firefox from the Mozilla Products page

This will address the following 13 issues:

•Mozilla Firefox Multiple Vulnerabilities Fixed in 3.0.7 (mozilla-firefox-mfsa-2009-07-to-2009-11)

•Mozilla Firefox Multiple Vulnerabilities Fixed in 3.0.8 (mozilla-firefox-mfsa-2009-12-to-2009-13)
•2 instances of Mozilla Firefox CSS Reference Counter Code Execution Vulnerability (windows-mozilla-firefox-css-reference-counter-code-exec)
•2 instances of Mozilla Firefox Multiple Vulnerabilities Fixed in versions 2.0.0.17 and 3.0.2 (windows-mozilla-firefox-multiple-vulns-2-0-0-17-and-3-0-2)
•2 instances of Mozilla Firefox Multiple Vulnerabilities Fixed in versions 2.0.0.18 and 3.0.4 (windows-mozilla-firefox-multiple-vulns-2-0-0-18-and-3-0-4)
•2 instances of Mozilla Firefox Multiple Vulnerabilities Fixed in versions 2.0.0.19 and 3.0.5 (windows-mozilla-firefox-multiple-vulns-2-0-0-19-and-3-0-5)
•Multiple Mozilla Firefox Vulnerabilities Fixed in Version 2.0.0.12 (windows-mozilla-multiple-vulns-2008-12)
•Multiple Mozilla Firefox Vulnerabilities: Fixed in 2.0.0.13 (windows-mozilla-multiple-vulns-2008-13)
•Multiple Mozilla Firefox Vulnerabilities Fixed in version 2.0.0.15 (windows-mozilla-multiple-vulns-2008-15)

Upgrade to the latest version of Wireshark

Estimated time: 10 minutes
Download and apply the upgrade from: http://www.wireshark.org/download/src/all-versions/wireshark-1.2.1.tar.bz2
As of July 2009, the latest version of Wireshark is 1.2.1, released on July 20, 2009.

This will address the following 10 issues:
•Wireshark Multiple Vulnerabilities in Bluetooth ACL, Q.931, Tamos CommView, USB, PRP and MATE dissectors (wireshark-bluetooth-q931-tamos-usb-prp-mate-vulns)
•Wireshark Multiple Vulnerabilities in GSM SMS, PANA, KISMET, RTMPT, RMI, SS7 MSU (wireshark-gsm-pana-kismet-rtmpt-rmi-ss7-vulns)
•Wireshark Multiple Vulnerabilities in NCP, zlib, Tektronix rf5 parsers (wireshark-ncp-zlib-rf5-vulns)
•Wireshark NetScreen Snoop Capture File Buffer Overflow Vulnerability (wireshark-netscreen-snoop-capture-file-bof)
•Wireshark Packet Reassembly Denial of Service (wireshark-packet-reassembly-dos)
•Wireshark DoS Vulnerabilities in SCCP, LDAP, Roofnet, X509sat Dissectors (wireshark-sccp-ldap-roofnet-x509sat-dissectors-dos)
•Wireshark DoS Vulnerabilities in SCTP, SNMP, TFTP Dissectors (wireshark-sctp-snmp-tftp-dissectors-dos)
•Wireshark Multiple Vulnerabilities Fixed in version 1.0.7 (wireshark-wnpa-sec-2009-02)
•Wireshark Vulnerability Fixed in version 1.0.8 (wireshark-wnpa-sec-2009-03)
•Wireshark Multiple Vulnerabilities Fixed in version 1.2.1 (wireshark-wnpa-sec-2009-04)

Follow the instructions from Microsoft KB973472.

Estimated time: 2 hours
Microsoft has issued an advisory regarding this issue and has offered a workaround.

This will address the following issue: Microsoft Office Web Components Code Execution Vulnerability (microsoft-office-web-components-activex).

Follow the instructions from Microsoft KB972890.

Estimated time: 2 hours
Microsoft has issued
an advisory regarding this issue and has offered a workaround.

This will address the following issue: Microsoft DirectShow Streaming Video ActiveX Control Buffer Overflow (activex-directshow-video-buffer-overflow).

Apply the security policy to the system

Estimated time: 1 hour
If you are configuring a standalone computer or domain member, apply the security policy to the system using the Security Configuration and Analysis MMC add-in.

1. Click Start, and then click Run.
2. In the Open box, type mmc, and then click OK.
3. On the Console menu, click Add/Remove Snap-in.
4. In the Add/Remove Snap-in dialog box, click the Standalone tab, and then click Add.
5. In the Add Standalone Snap-in dialog box, click Security Configuration and Analysis, click Add, click Close, and then click OK.
6. In the Security Configuration and Analysis snap-in, right click on Security Configuration and Analysis. Click Open Database and type a new database name.
7. After typing the new database name, you will be prompted to choose the security template to import into this database. Browse to the security policy template (INF) file and click Open.
8. In the Security Configuration and Analysis snap-in, right click on Security Configuration and Analysis. Click Configure Computer Now.
   If you are configuring security for an entire domain, use the Domain Security Policy tool.

1. Log on to the Domain Controller with an account that has administrative rights.
2. Copy the desired template into the \%Systemroot%\Security\Templates (or C:\WINNT\Security\Templates) folder of the system partition.
3. Click Start, point to Programs, point to Administrative Tools, and then click Domain Security Policy. This opens the Domain Security Policy console.
4. In the console tree, right-click Security Settings.
5. Click Import Policy.
6. Find and select the security configuration template so that it appears in the File name: text box. Check the Clear this database check box and click the Open button.
7. Close the Domain Security Policy.
   If you are configuring security for a domain controller, use the Domain Controller Security Policy tool.

1. Log on to the Domain Controller with domain account that has domain administrative rights.
2. Copy the desired template into the \%Systemroot%\Security\Templates (or C:\WINNT\Security\Templates) folder of the system partition.
3. Click Start, point to Programs, point to Administrative Tools, and then click Domain Controller Security Policy. This opens the Domain Controller Security Policy console.

4. In the console tree, right-click Security Settings.
5. Click Import Policy.
6. Find and select the security configuration template so that it appears in the File name: text box. Check the Clear this database check box and click the Open button.
7. Reboot the Domain Controller.

This will address the following issue: Windows security policy violation (windows-security-policy-violation).

Disable LANMAN Authentication In Samba

Estimated time: 15 minutes

Add the following line in the smb.conf's global section:

```
lanman auth = No
```

This will address the following issue: Weak LAN Manager hashing permitted (CIFS-GENERIC-0005).

Upgrade the CIFS authentication method

Estimated time: 15 minutes

Upgrade the authentication method using the registry. Note that upgrading the authentication method to NTMLv2 will break compatibility with Windows 95/98/ME systems and older pre-NT4 SP4 systems. This behavior is by design. If the system itself is NT4 SP3 or earlier, it must be upgraded to at least NT4 SP4 before making these changes. Note that the settings described below can also be set via Group Policy, under "Security Options", "LAN Manager Authentication Level".

Run the registry editor (regedit.exe or regedt32.exe) and browse to the following key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
```

and set the following value:

```
Value Name: LMCompatibilityLevel
Data Type: REG_DWORD
Data:  At least level 3 should be used, preferably level 5.
```

The valid values are:

0	Send LM response and NTLM response; never use NTLMv2 session security
1	Use NTLMv2 session security if negotiated
2	Send NTLM authenication only
3	Send NTLMv2 authentication only
4	DC refuses LM authentication
5	DC refuses LM and NTLM authenication (accepts only NTLMv2)

You should also modify the following values to the highest levels:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\
Value Name: NtlmMinClientSec
     Data Type: REG_DWORD
```

Data: See

Q147706 (http://support.microsoft.com/default.aspx?scid=kb;EN-US;147706) for details.
Value Name: NtlmMinServerSec
Data Type: REG_DWORD
Data: See

Q147706 (http://support.microsoft.com/default.aspx?scid=kb;EN-US;147706) for details.
You must then shut down and restart for the changes to take effect.

This will address the following issue: Weak LAN Manager hashing permitted (CIFS-GENERIC-0005).

Fix Windows administrative shares enabled

Estimated time: 15 minutes
Open your registry editor (regedit.exe) and browse to:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer

•Make sure the "Start" REG_DWORD value is set to 3.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

•Make sure the "AutoShareServer" REG_DWORD value is set to 0.
•Make sure the "AutoShareWks" REG_DWORD value is set to 0 (not required under Win2k and later).

This will address the following issue: Windows administrative shares enabled (WINDOWS-AUTO-SHARES).

Download and install update 950582 or 953252 or 967715

Estimated time: 1 hour
Download and apply the patch from: http://support.microsoft.com/kb/967715
Install one of the 3 updates documented in Microsoft Knowledge Base article 967715, that is security update 950582, or update 953252, or update 967715.

This will address the following issue: Microsoft KB967940: Correct "Disable Autorun Registry Key" Enforcement (windows-correct-autorun-disable).

Fix Windows display last username enabled

Estimated time: 15 minutes
For all versions of Windows NT and Windows 2000/XP, you must take the following steps. Note that on Windows 2000, you must follow both steps 1 AND 2 -- there are two separate registry entries which must be set.

1. Open your registry editor (regedit.exe) and browse to the following registry key:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
   Ensure that the "DontDisplayLastUserName" REG_SZ value is set to "1". Please note that this is a REG_SZ (string) value, not a DWORD.
2. Then, if you are running Windows 2000 or later, browse to the following registry key:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Ensure that the "DontDisplayLastUserName" REG_DWORD value is set to "1". Please note that this is indeed a REG_DWORD value, not a string.

In Windows 2000, this particular registry entry can be modified via the Local Security Policy control panel. Go to Administrative Tools, Local Security Policy. Expand the Local Policies folder, and choose the Security Options folder. Select the option titled "Do not display last user name in logon screen" and change it to "Enabled".

NOTE: Disabling the last username display will cause the Autologin feature not to work. However, the autologin feature is poses serious security risks itself and therefore should be disabled as well. See Microsoft Knowledge Base article Q159969 - AutoLogon Fails If DontDisplayLastUserName Is Also Enabled (http://support.microsoft.com/support/kb/articles/q159/9/69.asp) for more information.

This will address the following issue: Windows display last username enabled (WINDOWS-DISPLAY-LAST-USERNAME).

Fix Printer driver installation is not restricted

Estimated time: 15 minutes

1. Open the registry editor and browse to the following key:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers`
   This registry key will not exist if printers have not yet been installed. In this case, you must create this registry key before continuing.
2. Under this key, add a DWORD value named "AddPrinterDrivers" and set it to 1. This will restrict the ability to install printer drivers to Administrators only (for servers) or to both Power Users and Administrators (for workstations).

This will address the following issue: Printer driver installation is not restricted (windows-unrestricted-printer-drivers).

Fix the Windows XP firewall settings

Estimated time: 15 minutes

To fix the firewall settings, follow these steps:

1. Go to Windows Control Panel and select Windows Firewall.
2. Select the 'ON' radio button and Check the 'Don't Allow Exceptions' checkbox.
3. Go to the exceptions tab
4. Check the 'Display notification when Windows Firewall blocks a program' checkbox.

Certain worms and trojans have been known to modify the firewall settings. Perform a complete scan to make sure that the system is not infected.

This will address the following issue: Windows XP firewall settings are unsafe (xp-unsafe-firewall-settings).

Fix the following Security Center settings

Estimated time: 15 minutes

Take following steps to change each of the above settings:

• To change 'AntiVirusDisableNotify', 'FirewallDisplayNotify' and 'UpdatesDisableNotify'

1. Go to Control Panel and select Security Center
2. In the 'Resources' section located on the upper left quadrant of the security center console, select 'Change the way Security Center alerts me'

3. Check all the three checkboxes and click 'OK'

• To change 'AntiVirusOverride' entry:

1. Go to Control Panel and select Security Center
2. In the Virus Protection section, click on 'Recommendations' (if present)
3. Uncheck the checkbox at the bottom of the dialog box(I have an antivirus program that I'll monitor myself) and press 'OK'.

• To Change 'FirewallOverride' entry:

1. Go to Control Panel and select Security Center
2. In the Firewall section, click on 'Recommendations' (if present)
3. Uncheck the checkbox at the bottom of the dialog box(I have a firewall solution that I'll monitor myself) and press 'OK'.

It may be possible that the above settings were changed unintentionally or by a worm or spyware. Please perform a complete scan to make sure that the system is not infected.

This will address the following issue: Windows XP Security Center settings are unsafe (xp-unsafe-security-center-settings).

3.1.3. For Microsoft Internet Explorer 6.0 SP2 on Microsoft Windows XP Professional SP2

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 30 minutes.

Download and install Microsoft patch WindowsXP-KB974455-x86-ENU.exe (4977008 bytes)

Estimated time: 30 minutes

Microsoft Internet Explorer >= 6.0 and < 7.0 on Microsoft Windows XP Professional SP3 OR SP2 (x86), Microsoft Windows XP Home SP3 OR SP2 (x86)

Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2009/10/windowsxp-kb974455-x86-enu_99bebe04a5b465074fa6ea015beac00bb9290bd4.exe

This will address the following 4 issues:

•MS08-078: Security Update for Internet Explorer (WINDOWS-HOTFIX-MS08-078)

•MS09-014: Cumulative Security Update for Internet Explorer (WINDOWS-HOTFIX-MS09-014)

•MS09-019: Cumulative Security Update for Internet Explorer (WINDOWS-HOTFIX-MS09-019)

•MS09-034: Cumulative Security Update for Internet Explorer (WINDOWS-HOTFIX-MS09-034)

3.1.4. For Microsoft Office 2003 11.0.5614.0

These vulnerabilities can be resolved by performing the following 3 steps. The total estimated time to perform all of these steps is 1 hour.

Download and install Microsoft patch OWC102003SP3.CAB (5844833 bytes)

Estimated time: 20 minutes

Microsoft Office 2003

Download and apply the upgrade from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/owc102003sp3_03116dd8122fbadaa38d40767a6d92678126e557.cab

NOTE: Microsoft Windows Installer is required to install this patch.

This will address the following issue: MS07-042: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227) (WINDOWS-HOTFIX-MS07-042).

Download and install Microsoft patch GDIPLUS.CAB (1295779 bytes)

Estimated time: 20 minutes

Microsoft Office 2003

Download and apply the patch from:

http://download.windowsupdate.com/msdownload/update/software/secu/2009/10/gdiplus_32bfcbdf39ffc80a7a599bc807e77a9a914e6d47.cab

NOTE: Microsoft Windows Installer is required to install this patch.

This will address the following issue: MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution (954593) (WINDOWS-HOTFIX-MS08-052).

Download and install Microsoft patch MAINSP3.CAB (113491064 bytes)

Estimated time: 20 minutes

Microsoft Office 2003

Download and apply the upgrade from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/mainsp3_8dec796cbac8915e6987e7405b3a9910c0a9a1b7.cab

NOTE: Microsoft Windows Installer is required to install this patch.

This will address the following issue: Office 2003 Service Pack 3 (SP3) (servicepack-office-2003-sp3).

3.2. Remediation Plan for 10.2.51.250 (iml-accounting)

3.2.1. For Oracle 10.1.0.3.0.0

These vulnerabilities can be resolved by performing the following 3 steps. The total estimated time to perform all of these steps is 5 hours 15 minutes.

Apply the October 2009 Critical Patch Update (CPU) for Oracle

Estimated time: 2 hours

The October 2009 CPU should be applied to the Oracle database. A table containing the list of available CPUs and patch sets is listed on the Oracle security alert website. Oracle does not make patch sets available to the public. A metalink account is required to access patch downloads. The specific download link for this patch set may be located on Metalink, with doc id 881382.1.

This will address the following 29 issues:

•Oracle DBMS_AQADM_SYS SQL Injection (oracle-dbms_aqadm_sys-sql-injection)

•Oracle DBMS_CAPTURE_ADM_INTERNAL Buffer Overflow (oracle-dbms_capture_adm_internal-bof)

•Oracle DBMS_CDC_IPUBLISH Buffer Overflow (oracle-dbms_cdc_ipublish-sql-injection-bof)

•Oracle DBMS_CDC_PUBLISH SQL Injection (oracle-dbms_cdc_publish-sql-injection)

•Oracle DBMS_LOGREP_UTIL Buffer Overflow (oracle-dbms_logrep_util-bof)

•Oracle DBMS_METADATA SQL Injection (oracle-dbms_metadata-get_ddl-sql-injection)

•Oracle DBMS_REPCAT_UNTRUSTED UNREGISTER_SNAPSHOT Buffer Overflow (oracle-dbms_repcat_untrusted-bof)

•Oracle DBMS_XDBZ ENABLE_HIERARCHY SQL Injection (oracle-dbms_xdbz-enable-hierarchy-sql-injection)

•Oracle DBMS_XMLSCHEMA Buffer Overflow (oracle-dbms_xmlschema-generateschema-bof)

•Oracle DBMS_XMLSCHEMA_INT Buffer Overflow (oracle-dbms_xmlschema_int-generateschema-bof)

•Oracle KUPM$MCP MAIN SQL Injection (oracle-kupm-mcp-main-sql-injection)
•Oracle KUPW$WORKER MAIN SQL Injection (oracle-kupwworker-main-sql-injection)
•Oracle MDSYS SDO_PRIDX SQL Injection (oracle-mdsys-sdo_pridx-sql-injection)
•Missing Oracle Critical Patch Update (CPU) for April 2005 (oracle-missing-april-2005-cpu)
•Missing Oracle Critical Patch Update (CPU) for April 2006 (oracle-missing-april-2006-cpu)
•Missing Oracle Critical Patch Update (CPU) for April 2007 (oracle-missing-april-2007-cpu)
•Missing Oracle Critical Patch Update (CPU) for April 2008 (oracle-missing-april-2008-cpu)
•Missing Oracle Critical Patch Update (CPU) for January 2007 (oracle-missing-jan-2007-cpu)
•Missing Oracle Critical Patch Update (CPU) for January 2008 (oracle-missing-jan-2008-cpu)
•Missing Oracle Critical Patch Update (CPU) for July 2006 (oracle-missing-july-2006-cpu)
•Missing Oracle Critical Patch Update (CPU) for October 2005 (oracle-missing-oct-2005-cpu)
•Missing Oracle Critical Patch Update (CPU) for October 2006 (oracle-missing-oct-2006-cpu)
•Missing Oracle Critical Patch Update (CPU) for October 2007 (oracle-missing-oct-2007-cpu)
•Missing Oracle Critical Patch Update (CPU) for October 2008 (oracle-missing-oct-2008-cpu)
•Oracle SDO_IDX CMT_IDX_CHNGS SQL Injection (oracle-sdo_idx-cmt_idx_chngs-sql-injection)
•Oracle SDO_TUNE EXTENT_OF SQL Injection (oracle-sdo_tune-extent-of-sql-injection)
•Oracle LT FINDRICSET SQL Injection (oracle-sys_lt_findricset-sql-injection)
•Oracle SYS.LTADM AreThereDiffs SQL Injection (oracle-wmsys-ltadm-aretherediffs-sql-injection)
•Oracle XDB.XDB_PITRIG_PKG PITRIG_DROP and PITRIG_TRUNCATE Procedure Vulnerabilities (oracle-xdb-pitrig_pkg-procedures-inj-bof)

Revoke permissions on vulnerable packages to mitigate impact

Estimated time: 15 minutes

Execute permissions for specific packages may be revoked from untrusted users by running the following command on the Oracle server as a DBA. `REVOKE EXECUTE ON <SCHEMA>.<PACKAGENAME> FROM <USER|GROUP> FORCE;`

Where PACKAGENAME is the name of a vulnerable package, SCHEMA is the schema which the package resides in, and USER|GROUP is a user or group (role). If the package is owned by a different user, Oracle DBMS may respond with an error resembling "cannot REVOKE privileges you did not grant." In such a case, the revoke statement needs to be executed as the owner (schema) of the package. The owner of the package may be discovered via: `SELECT OWNER FROM TABLE_PRIVILEGES WHERE TABLE_NAME='<PACKAGENAME>'`

The result of this command may then be used in a subsequent ALTER SESSION statement to switch to that schema/user: `ALTER SESSION SET CURRENT_SCHEMA='<OWNER>'`

Where OWNER was the value retrieved in the previous statement. It should then be possible to reissue the revoke statement above to secure the vulnerable package(s).

For example, to revoke the execute privilege on the DBMS_SYS_SQL package group PUBLIC, which typically contains all users, one may execute: `REVOKE EXECUTE ON SYS.DBMS_SYS_SQL FROM PUBLIC FORCE;`

Likewise, to revoke the execute privilege on the same package from user SCOTT, one may execute: `REVOKE EXECUTE ON SYS.DBMS_SYS_SQL FROM SCOTT FORCE;`

The current permissions granted for users and groups (roles) can be observed by executing the following as a DBA: `SELECT * FROM DBA_TAB_PRIVS WHERE TABLE_NAME='<PACKAGENAME>'`

Where PACKAGENAME is the name of a package (like DBMS_SYS_SQL, above).

Privilege tests can be performed on a per-user basis as well by executing the following as a logged in user: `SELECT * FROM TABLE_PRIVILEGES WHERE TABLE_NAME='<PACKAGENAME>'`
Each row returned describes a grant role for the current user.

This will address the following 18 issues:

•Oracle DBMS_AQADM_SYS SQL Injection (oracle-dbms_aqadm_sys-sql-injection)
•Oracle DBMS_CAPTURE_ADM_INTERNAL Buffer Overflow (oracle-dbms_capture_adm_internal-bof)
•Oracle DBMS_CDC_IPUBLISH Buffer Overflow (oracle-dbms_cdc_ipublish-sql-injection-bof)
•Oracle DBMS_CDC_PUBLISH SQL Injection (oracle-dbms_cdc_publish-sql-injection)
•Oracle DBMS_LOGREP_UTIL Buffer Overflow (oracle-dbms_logrep_util-bof)
•Oracle DBMS_METADATA SQL Injection (oracle-dbms_metadata-get_ddl-sql-injection)
•Oracle DBMS_REPCAT_UNTRUSTED UNREGISTER_SNAPSHOT Buffer Overflow (oracle-dbms_repcat_untrusted-bof)
•Oracle DBMS_XDBZ ENABLE_HIERARCHY SQL Injection (oracle-dbms_xdbz-enable-hierarchy-sql-injection)
•Oracle DBMS_XMLSCHEMA Buffer Overflow (oracle-dbms_xmlschema-generateschema-bof)
•Oracle DBMS_XMLSCHEMA_INT Buffer Overflow (oracle-dbms_xmlschema_int-generateschema-bof)
•Oracle KUPM$MCP MAIN SQL Injection (oracle-kupm-mcp-main-sql-injection)
•Oracle KUPW$WORKER MAIN SQL Injection (oracle-kupwworker-main-sql-injection)
•Oracle MDSYS SDO_PRIDX SQL Injection (oracle-mdsys-sdo_pridx-sql-injection)
•Oracle SDO_IDX CMT_IDX_CHNGS SQL Injection (oracle-sdo_idx-cmt_idx_chngs-sql-injection)
•Oracle SDO_TUNE EXTENT_OF SQL Injection (oracle-sdo_tune-extent-of-sql-injection)
•Oracle LT FINDRICSET SQL Injection (oracle-sys_lt_findricset-sql-injection)
•Oracle SYS.LTADM AreThereDiffs SQL Injection (oracle-wmsys-ltadm-aretherediffs-sql-injection)
•Oracle XDB.XDB_PITRIG_PKG PITRIG_DROP and PITRIG_TRUNCATE Procedure Vulnerabilities (oracle-xdb-pitrig_pkg-procedures-inj-bof)

Upgrade to a supported version and patch set of Oracle

Estimated time: 3 hours
Upgrade to a supported version and patch set of the Oracle database system.

This will address the following issue: Oracle Obsolete Version (oracle-obsolete-version).

3.2.2. For OpenSSH 4.3p2

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 2 hours 30 minutes.

Upgrade to the latest version of OpenSSH

Estimated time: 2 hours 30 minutes
The latest version of OpenSSH is 5.2 (OpenBSD source) and 5.2p1 (portable source), both released on February 22, 2009.
While you can always build OpenSSH from source, many platforms and distributions provide pre-built binary packages for OpenSSH. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

This will address the following 4 issues:

•OpenSSH X11 Cookie Local Authentication Bypass Vulnerability (openssh-x11-cookie-auth-bypass)
•OpenSSH CBC Mode Information Disclosure Vulnerability (ssh-openssh-cbc-mode-info-disclosure)
•OpenSSH X11 Fowarding Information Disclosure Vulnerability (ssh-openssh-x11-fowarding-info-disclosure)
•OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability (ssh-openssh-x11uselocalhost-x11-forwarding-session-hijack)

3.2.3. General

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 2 hours.

Apply the October 2009 Critical Patch Update (CPU) for Oracle

Estimated time: 2 hours

The October 2009 CPU should be applied to the Oracle database. A table containing the list of available CPUs and patch sets is listed on the Oracle security alert website. Oracle does not make patch sets available to the public. A metalink account is required to access patch downloads. The specific download link for this patch set may be located on Metalink, with doc id 881382.1.

This will address the following issue: Missing Oracle Critical Patch Update (CPU) for October 2009 (oracle-missing-oct-2009-cpu).