This package contains: CPSECPEP009S Version 1.1 Date: Nov 14/2007

1. PEP Number: CPSECPEP009S Version 1.1

Summary:

a). List of CRs resolved in this PEP, section 3.1
b). List of hotfixes installed by this PEP, section 3.2
c). List of registry changes, section 3.3
d). List of services being disabled, section 3.4
e). Opsware related info, section 9
f). New hotfix checker, section 10

2. Problem Description

This package contains Microsoft hotfixes to be installed on a CallPilot 3.0, 4.0 or 5.0 server. Certain additional OS hardening and enhancement are also made to improve security.

The PEP contains all applicable hotfixes from the time Windows Server 2003 SP1 was originally released up to and including Nov 13th, 2007 (Up to MS07-062 but excluding IE7 and SP2). It is intended for installation on a system that has either Service Pack 1 or Service Pack 2 installed.

This PEP will need about 250 MB ~ 500 MB on C: to start installation process, actual disk space consumption is less than 250 MB.

Installation can take up to 50 minutes depending on your platform and CallPilot release. Less time is needed if anti-virus software is temporarily disabled during installation. This PEP may be installed remotely using pcAnywhere or Remote Desktop.

NOTE: Do not apply this security PEP CPSECPEP009S to CallPilot 4 servers which have already been JITC hardened since the PEP may weaken some of the security hardening needed for JITC compliance.

3.1 List of CRs that are fixed by this PEP

Q01367189 - Excessive TCP Keep-Alive LAN traffic with Desktop Messaging
Q01449531 - DMI view update sets CPservices to disabled after installing PEP CP202SEC004S
Q01617017 - MSI-Format support for CallPilot
Q01638452 - CP40404SU04S failed to install on a 703t with CallPilot 4.0 GA
Q01637569 - Receiving numerous event 59 and 32 in system log

3.2 list of hotfixes to patch the following Microsoft Bulletins

MS05-026 Jun 14/2005 Vulnerability in HTML Help Could Allow Remote Code Execution (896358)
MS05-027 Jun 14/2005 Vulnerability in Server Message Block Could Allow Remote Code Execution (896422)
MS05-028 Jun 14/2005 Vulnerability in Web Client Service Could Allow Remote Code Execution (896426)
MS05-033 Jun 14/2005 Vulnerability in Telnet Client Could Allow Information Disclosure (896428)
MS05-036 Jul 12/2005 Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (901214)
MS05-039 Aug 8/2005 Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)

MS05-040 Aug 8/2005 Vulnerability in Telephony Service Could Allow Remote Code Execution (893756)
MS05-041 Aug 8/2005 Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (899591)
MS05-042 Aug 8/2005 Vulnerabilities in Kerberos Could Allow Denial of Service, Information Disclosure, and Spoofing (899587)
MS05-045 Oct 11/2005 Vulnerability in Network Connection Manager Could Allow Denial of Service (905414)
MS05-046 Oct 11/2005 Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589)
MS05-048 Oct 11/2005 Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution (901017)
MS05-049 Oct 11/2005 Vulnerabilities in Windows Shell Could Allow Remote Code Execution (900725)
MS05-050 Oct 11/2005 Vulnerability in DirectShow Could Allow Remote Code Execution (904706)
MS05-051 Oct 11/2005 Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)
MS05-052 Oct 11/2005 Cumulative Security Update for Internet Explorer (896688)
MS06-002 Jan 10/2006 Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution (908519)
MS06-006 Feb 14/2006 Vulnerability in Windows Media Player Plug-in with Non-Microsoft Internet Browsers Could Allow Remote Code Execution (911564)
MS06-007 Feb 14/2006 Vulnerability in TCP/IP Could Allow Denial of Service (913446)
MS06-008 Feb 14/2006 Vulnerability in Web Client Service Could Allow Remote Code Execution (911927)
MS06-013 Apr 11/2006 Cumulative Security Update for Internet Explorer (912812)
MS06-014 Apr 11/2006 Vulnerability in the Microsoft Data Access Components (MDAC) Function Could Allow Code Execution (911562)
MS06-015 Apr 11/2006 Vulnerability in Windows Explorer Could Allow Remote Code Execution (908531)
Dec 12/2005 Update for Windows Server 2003 (KB910437)

MS06-022 Jul 26/2006 Vulnerability in ART image rendering could allow remote code execution (918439)
MS06-023 Jul 26/2006 Vulnerability in Microsoft JScript could allow remote code execution (917344)
MS06-024 Jul 26/2006 Vulnerability in Windows Media Player could allow remote code execution (917734)
MS06-030 Jul 26/2006 Vulnerability in Server Message Block could allow elevation of privilege (914389)
MS06-032 Jul 26/2006 Vulnerability in TCP/IP could allow remote code execution (917953)
MS06-034 Jul 26/2006 Vulnerability in Internet Information Services that use Active Server Pages could allow remote code execution (917537)
MS06-035 Jul 26/2006 Vulnerability in Server service could allow remote code execution (917159)
MS06-025 Aug 8/2006 Vulnerability in Routing and Remote Access could allow remote code execution (911280)
MS06-036 Aug 30/2006 A vulnerability in the DHCP Client Service could allow remote code execution (914388)
MS06-041 Aug 30/2006 Vulnerability in DNS resolution could allow remote code execution (920683)

MS06-043 Aug 30/2006 Vulnerability in Microsoft Windows could allow remote code execution (920214)
MS06-046 Aug 30/2006 Vulnerability in HTML Help could allow remote code execution (922616)
MS06-050 Aug 30/2006 Vulnerabilities in Microsoft Windows Hyperlink Object Library could allow remote code execution (920670)
MS06-040 Sep 12/2006 Vulnerability in Server service could allow remote code execution (921883)
MS06-053 Sep 12/2006 Vulnerability in Indexing Service could allow cross-site scripting (920685)
Sep 09/2006 Update for Windows Server 2003 (KB922582)
MS06-057 Oct 10/2006 Vulnerability in Windows Explorer Could Allow Remote Execution (923191)
MS06-061 Oct 10/2006 Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (924191)
MS06-063 Oct 10/2006 Vulnerability in Server Service Could Allow Denial of Service and Remote Code Execution (923414)
MS06-064 Oct 10/2006 Vulnerabilities in TCP/IP IPv6 Could Allow Denial of Service (922819)
MS06-065 Oct 10/2006 Vulnerability in Windows Object Packager Could Allow Remote Execution (924496)
MS06-066 Nov 14/2006 Vulnerabilities in Client Service for NetWare Could Allow Remote Code Execution (923980)
MS06-068 Nov 14/2006 Vulnerability in Microsoft Agent Could Allow Remote Code Execution (920213)
MS06-074 Dec 12/2006 Vulnerability in SNMP Could Allow Remote Code Execution (926247)
MS06-075 Dec 12/2006 Vulnerability in Windows Could Allow Elevation of Privilege (926255)
MS06-076 Dec 12/2006 Cumulative Security Update for Outlook Express (923694)
MS06-078 Dec 12/2006 Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689)

MS07-004 Jan 09/2007 Vulnerability in Vector Markup Language Could Allow Remote Code Execution (929969)
MS07-006 Feb 13/2007 Vulnerability in Windows Shell Could Allow Elevation of Privilege (928255)
MS07-008 Feb 13/2007 Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843)
MS07-011 Feb 13/2007 Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution (926436)
MS07-012 Feb 13/2007 Vulnerability in Microsoft MFC Could Allow Remote Code Execution (924667)
MS07-013 Feb 13/2007 Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution (918118)
MS07-016 Feb 13/2007 Cumulative Security Update for Internet Explorer (928090)
MS07-017 Apr 03/2007 Vulnerabilities in GDI Could Allow Remote Code Execution (925902)
MS07-020 Apr 10/2007 Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168)
MS07-021 Apr 10/2007 Vulnerabilities in CSRSS Could Allow Remote Code Execution (930178)
MS07-022 Apr 10/2007 Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784)

MS07-031 Jun 12/2007 Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840)
MS07-033 Jun 12/2007 Cumulative Security Update for Internet Explorer (933566)
MS07-034 Jun 12/2007 Cumulative Security Update for Outlook Express and Windows Mail (929123)
MS07-035 Jun 12/2007 Vulnerability in Win 32 API Could Allow Remote Code Execution (935839)

MS07-039 Jul 10/2007 Vulnerability in Windows Active Directory Could Allow Remote Code Execution (926122)
MS07-040 Jul 10/2007 Vulnerabilities in .NET Framework Could Allow Remote Code Execution (931212)

MS07-042 Aug 14/2007 Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227)
MS07-043 Aug 14/2007 Vulnerability in OLE Automation Could Allow Remote Code Execution (921503)
MS07-045 Aug 14/2007 Cumulative Security Update for Internet Explorer (937143)
MS07-046 Aug 14/2007 Vulnerability in GDI Could Allow Remote Code Execution (938829)
MS07-047 Aug 14/2007 Vulnerabilities in Windows Media Player Could Allow Remote Code Execution (936782)
MS07-050 Aug 14/2007 Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)

MS07-056 Oct 9/2007 Security Update for Outlook Express and Windows Mail (941202)
MS07-057 Oct 9/2007 Cumulative Security Update for Internet Explorer (939653)
MS07-058 Oct 9/2007 Vulnerability in RPC Could Allow Denial of Service (933729))

MS07-061 Nov 13/2007 Vulnerability in Windows URI Handling Could Allow Remote Code Execution (943460)
MS07-028 Vulnerability in CAPICOM Could Allow Remote Code Execution 931906

KB890830 Windows Malicious Software Removal Tool
KB910437 Windows Automatic Update, access violation error
KB911897 Files corrupted on Windows Server 2003-based computer when you try to use the local UNC path to copy the files
KB917275 Windows Rights Management Services Client with Service Pack 2
KB922582 Error message when you try to update a Microsoft Windows-based computer: “0x80070002”
KB931836 February 2007 cumulative time zone update for Microsoft Windows operating systems
KB927891 Update for Windows Installer (MSI)

3.3 Changing Registry settings for improved security

Set threshold for Windows disk full warning to 2 percent
Enable signatures on SMB
Disable updating of Last Access Time by NTFS
Disable automatic creation of 8.3 file names
Set Event Log sizes, retention policy and guest access

Remote Access Settings- disallow saving password, enable logging, and answer after 5 rings

Remote Access Settings- Authentication Retries 6, Time 2 min, auto disconnect 2 min, KeepConn 5 min

Set KeepAliveTime to 300,000 ms according to MS recommendation.

Disable AutoRun on all drives

Set ScreenSaver Grace Period to 0

Do not allow users to configure proxy settings

Prevent Internet Explorer from automatically downloading new software to update/upgrade itself

Ensure that software update shell notifications are enabled

Tighten the handling of temporary directories used by Terminal Services (Remote Desktop) sessions

Remove Installer Policies Key to ensure that no elevated privileges have been given to the Installer

Although the Posix subsystem was already disabled, remove an additional registry key associated with Posix

Remove the default password for use if autologin was configured from the registry

Enable SaveDLLSearchMode to make it harder for an attacker to introduce malicious software in the form of a DLL

Disable Remote Desktop Sharing (as used by Microsoft conferencing products)

Use only machine settings (not per user) for IE Security Zone Settings

Tighten restrictions on Remote Desktop Connections

Prevent the installation of Microsoft Messenger Client

Disable PCHealth Error Reporting to Microsoft

Prohibit the use of Internet Connection Sharing

Block the installation of Kernel Mode Printer drivers (most printer drivers are not kernel mode today)

Prevent Windows Media Player from automatically downloading and installing new codecs and updates

Disable Messenger Client and Messenger Service software

Registry flag changes to protect against a security issue with the Macromedia Flash Player

Workaround for MS06-041: Modifying the Autodial DLL within the Windows registry will prevent an application, specially crafted website or e-mail message from calling the affected API and exploiting the vulnerability.

Workaround for MS06-042: Disable caching of Web content in Internet Explorer

Disable the file: protocol handler

Internet Zone- Control Access to data sources across domains based on the site being browsed

Local Zone- Control Access to data sources across domains

Trusted Sites Zone- Control Access to data sources across domains

Restricted Sites Zone- Ensure Active Scripting has level of protection based on site being accessed

Trusted Sites Zone- Prevent execution of ActiveX controls not marked safe for scripting (prompt)

Local Zone- Prevent execution of ActiveX controls not marked safe for scripting (prompt)

Restricted Sites Zone- Prevent execution of ActiveX controls not marked safe for scripting

Internet Zone- Prevent execution of ActiveX controls not marked safe for scripting (prompt)

Restricted Sites Zone- Ensure Allow META REFRESH has level of protection based on the site being browsed

Internet Zone- Ensure paste operations via script have level of protection based on site being accessed

Local Zone- Ensure paste operations via script have level of protection based on site being accessed

Trusted Sites Zone- Ensure paste operations via script have level of protection based on site being accessed

Restricted Sites Zone- Ensure paste operations via script have level of protection based on site being accessed

Internet Zone- Ensure Display Mixed Content has level of protection based on the site being browsed

Restricted Sites Zone- Ensure Display Mixed Content has level of protection based on the site being browsed

Restricted Sites Zone- Ensure client certificates are not presented to web sites without the user’s acknowledgement

Internet Zone- Ensure client certificates are not presented to web sites without the user’s acknowledgement

Local Zone- Ensure client certificates are not presented to web sites without the user’s acknowledgement

Trusted Sites Zone- Ensure client certificates are not presented to web sites without the user’s acknowledgement

Internet Zone- Ensure Signed Active X controls cannot be downloaded

Local Zone- Ensure Signed Active X controls cannot be downloaded without prompt

Restricted Sites Zone- Ensure Signed Active X controls cannot be downloaded

Trusted Sites Zone- Ensure Signed Active X controls cannot be downloaded without prompt

Internet Zone- Ensure unsigned Active X controls cannot be downloaded

Restricted Sites Zone- Ensure unsigned Active X controls cannot be downloaded

Local Zone- Ensure unsigned Active X controls cannot be downloaded

Trusted Sites Zone- Ensure unsigned Active X controls cannot be downloaded

Restricted Sites Zone- Ensure Drag and Drop (and copy/paste) of files has level of protection based on the site being accessed

Internet Zone- Ensure Drag and Drop (and copy/paste) of files has level of protection based on the site being accessed

Ensure IE Error Reporting is disabled since it could send sensitive info to vendor

Restricted Sites Zone- Ensure file download is disabled

Internet Zone- prevent download of fonts without a prompt

Restricted Sites Zone- prevent download of fonts

Ensure user is warned when changing zones

Ensure user is warned when IE form data is redirected to another site

Local Zone- set to a custom level so other required settings can take effect

Restricted Sites Zone- set to a custom level so other required settings can take effect

Trusted Sites Zone- Ensure Trusted Sites zone is set to custom level

Ensure IE checks signatures on downloaded programs

Ensure IE warns of invalid certificates

Local Zone- Prevent execution of ActiveX controls not marked safe for scripting

Trusted Sites Zone- Prevent execution of ActiveX controls not marked safe for scripting (set to prompt)

Internet Zone- Prevent execution of ActiveX controls not marked safe for scripting (set to prompt)
Restricted Sites Zone- Prevent execution of ActiveX controls not marked safe for scripting (set to prompt)
Internet Zone- Prevent installation of desktop items
Local Zone- Prevent installation of desktop items without a prompt
Restricted Sites Zone- Prevent installation of desktop items
Trusted Sites Zone- Prevent installation of desktop items without a prompt
Local Zone- Set Java Permissions appropriate for Zone (prompt)
Internet Zone- Set Java Permissions appropriate for Zone
Trusted Sites Zone- Set Java Permissions appropriate for Zone
Restricted Sites Zone- Set Java Permissions appropriate for Zone
Local Zone- Control Launching Programs and files in IFRAME
Internet Zone- Control Launching Programs and files in IFRAME
Trusted Sites Zone- Control Launching Programs and files in IFRAME
Restricted Sites Zone- Control Launching Programs and files in IFRAME
Internet Zone- Control Frames trying to navigate across different domains
Restricted Sites Zone- Control Frames trying to navigate across different domains
Restricted Sites Zone- Control the running of ActiveX controls and plug-ins
Internet Zone- Control the scripting of Java applets (prompt)
Restricted Sites Zone- Control the scripting of Java applets
Internet Zone- Control Software Channel permissions
Local Zone- Control Software Channel permissions
Restricted Sites Zone- Control Software Channel permissions
Trusted Sites Zone- Control Software Channel permissions
Restricted Sites Zone- Control Submission of non-encrypted form data
Internet Zone- Control Submission of non-encrypted form data (prompt)
Restricted Sites Zone- User Authentication - Logon (control how credentials are passed to web sites)
Internet Zone- User Authentication - Logon (control how credentials are passed to web sites)
Local Zone- User Authentication - Logon (control how credentials are passed to web sites)
Trusted Sites Zone- User Authentication - Logon (control how credentials are passed to web sites)
Internet Zone- Control user data persistence
Restricted Zone- Control user data persistence
Prevent users from changing advanced settings in IE (commented out for CP5)

Enable Cipher setting for DES 56/56 for all protocols
Disable Cipher setting for NULL for all protocols (STIG says disable it, Beta Gold Disk says Enable it)
Enable Cipher setting for Triple DES 168/168 for all protocols
Enable Cipher setting for RC2 128/128 for all protocols
Enable Cipher setting for RC4 128/128 for all protocols
Enable Cipher setting for RC4 64/128 for all protocols
Enable Cipher setting for Skipjack for all protocols
Enable Cipher setting for NULL for all protocols
Enable MD5 and SHA Hashes for all protocols
Ensure IE SSL/TLS parameter allows SSL and TLS to be used from the browser
Disable Internet Printing Protocol

Set DCOM Static Allocation of Endpoints for NMAOS to ncacn_ip_tcp,0,5000 (always use port 5000)

3.4 Following services are set to disabled in order to reduce the attack surface

ALG
AppMgmt
Dfs
TrkWks
ERSvc
NtFrs
helpsvc
dmserver
WmdmPmSN
Spooler
RasAuto
RSoPProv
seclogon
ShellHWDetection
ScardSvr
sacsvr
Schedule
UPS
uploadmgr
vds
AudioSrv
WinHttpAutoProxySvc
WZCSVC
WebClient

4. Pre-installation notes

a). Make sure you are installing this PEP on a CallPilot 3.0, 4.0 or 5.0 server

This PEP replaces the following PEP if applicable:

- CP300SEC002S
- CP303SEC003S
- CP303SEC004S
- CP303SEC005S
- CP404SEC003S
- CP404SEC004S
- CP404SEC005S
- CPSECPEP006S
- CPSECPEP007S
- CPSECPEP008S

The replaced PEPs will be automatically removed from DMI Viewer when CPSECPEP009S is installed.

b). Make sure the CallPilot server is fully booted before beginning PEP installation.

Stop any other applications running on the local console, including all support tools and the CallPilot PEP Maintenance Utility (DMI Viewer).

c). Disable any active anti-virus software active on the server prior to installing this PEP. (This makes the PEP install faster.) As a precaution,

it's recommended the CLAN connection be disconnected prior to disabling the anti-virus software.

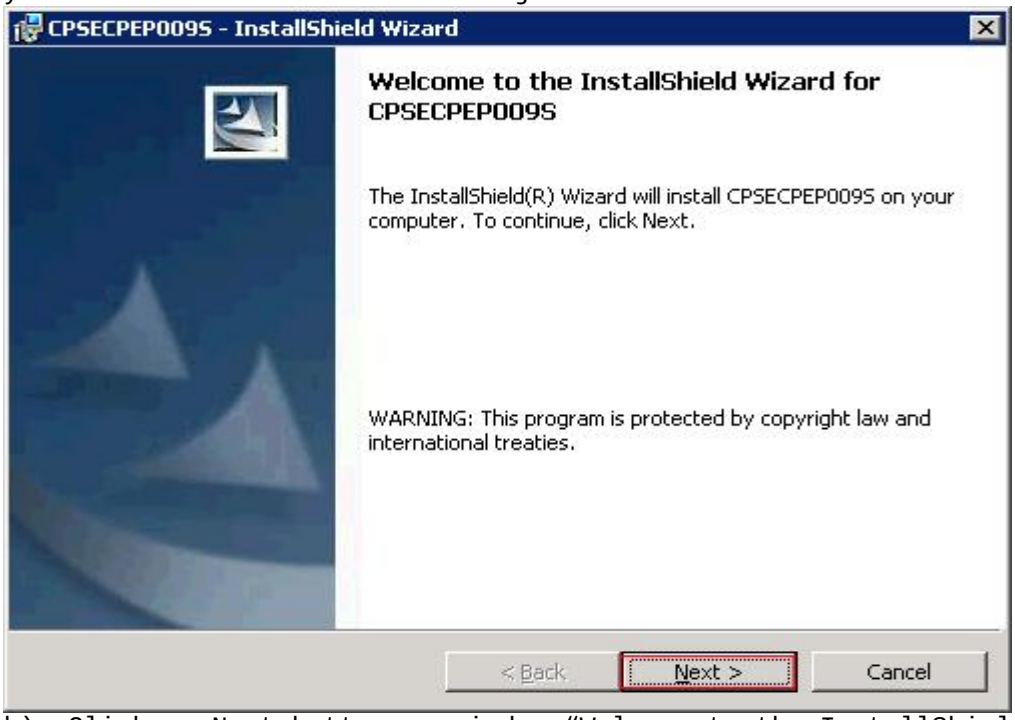
d). Ensure the system has sufficient disk-space available to install this PEP. If needed, remove any unnecessary files and folders in the c:\temp or d:\temp folders.
   If an error occurs while attempting to remove a particular file, ignore the error, but try to remove as many files and folders as possible in the temp folder. It is possible that the file is being used by Windows. Note: do not remove the c:\temp and d:\temp, and D:\TEMP\CPSECPEP009S folders. Once you have finished cleaning up, empty the recycle bin.

NOTE: This PEP will need about 250 MB ~ 500 MB on C: to start installation process, actual disk space consumption is less than 250 MB.

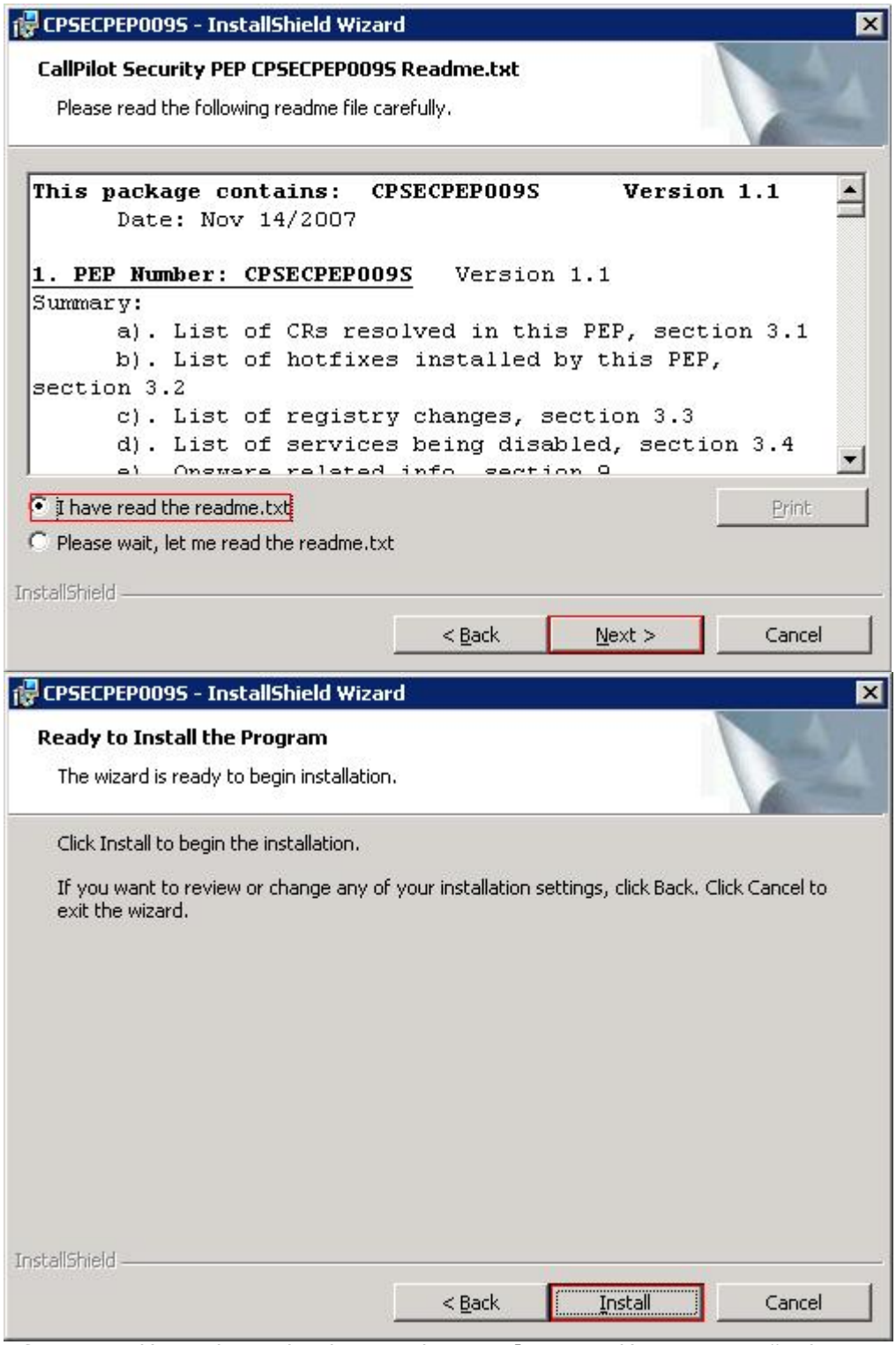
e). Ensure there is a recent backup available prior to installing this PEP. It's always recommended that a backup be performed (or split RAID) just prior to performing any server maintenance activity to ensure the most recent customer data is available should a restore be needed.

5. Installing the PEP

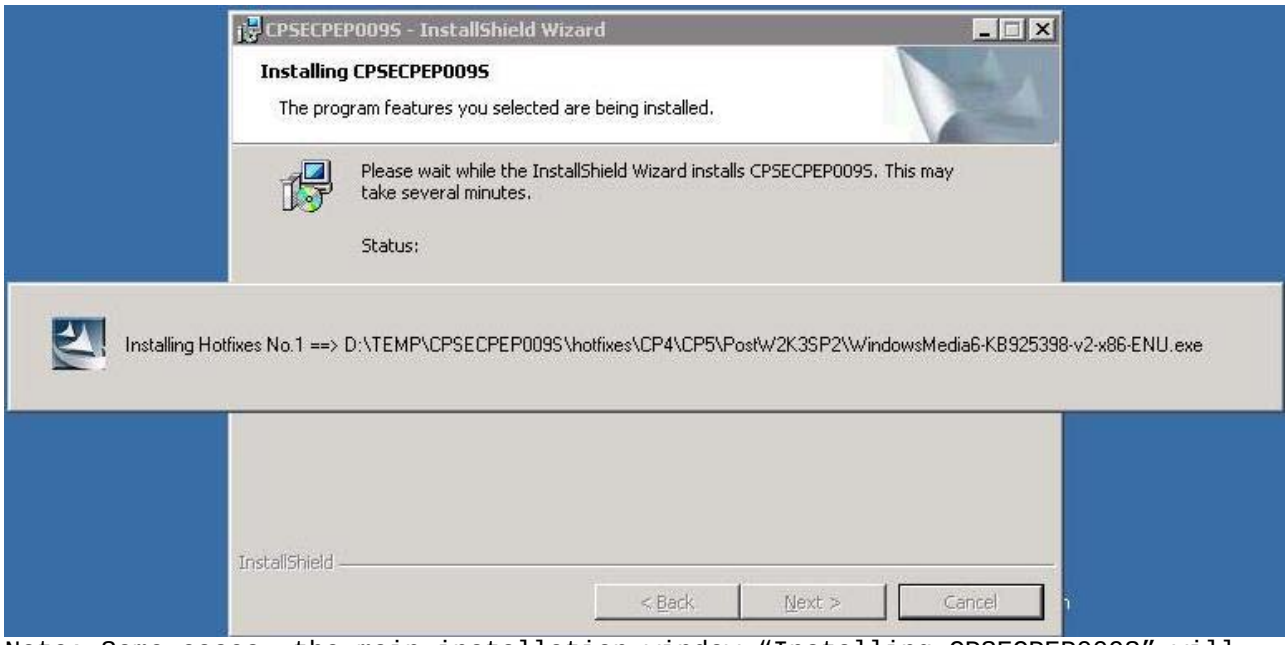
a). Begin installation by double-clicking on CPSECPEP009S.msi
NOTE: If you run the MSI from a network location (e.g. a shared network drive), you will get an “Open File – Security Warning” window asking that “Are you sure you want to run this software?” just click on the Run button to run it.



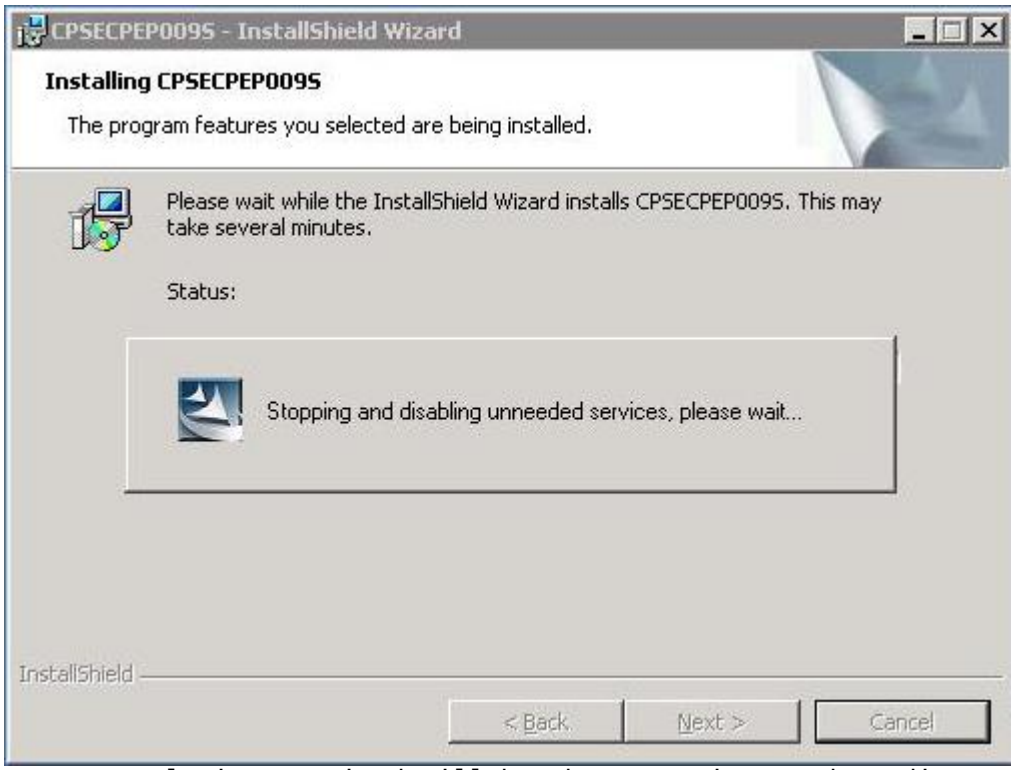
b). Click on Next button on window “Welcome to the InstallShield Wizard for CPSECPEP009S” and continue on to the Readme window.



After reading through the readme, select Radio Button “I have read the readme.txt” and click on Next button. On next window “Ready to install the Program”, click on Install button to install.

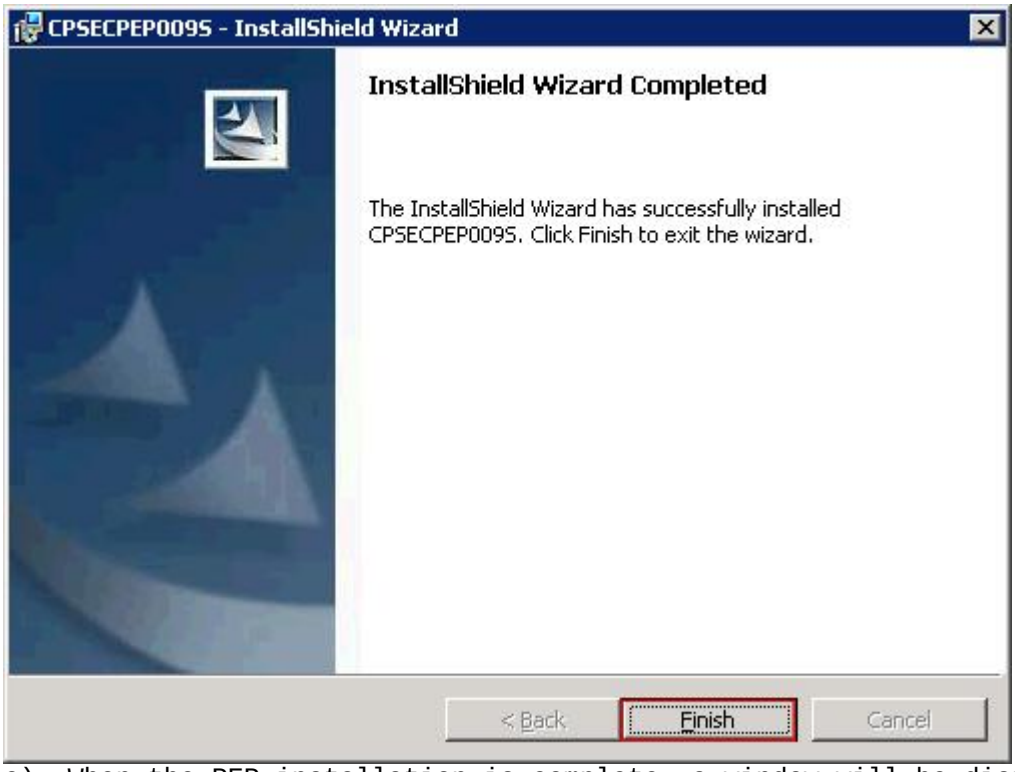


Note: Some cases, the main installation window “Installing CPSECPEP009S” will show up in front of the message box “Installing Hotfixes…”, that is a glitch of InstallShield, you may click on the message box and bring it to the front, either way will NOT affect the PEP install process.

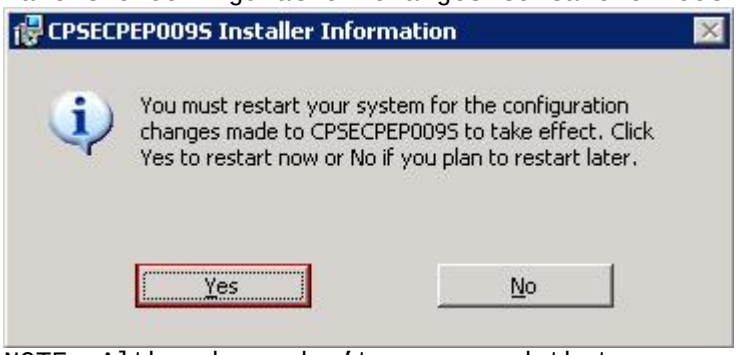


Note: Total time required will be about 50 minutes depending on your platform and CallPilot release, plus the time to reboot into service.

Note: This PEP automatically installs a number of Microsoft hot fixes. Do not close any windows or the PEP might not install successfully.



c). When the PEP installation is complete, a window will be displayed with the title "CallPilot OS Security PEP Installation Completed". Click on the Finish button to exit the wizard, and then you will be prompted for option Yes to restart the server now and No to restart at a later time. You need a reboot to make the configuration changes to take effect.



NOTE: Although we don’t recommend that you apply this PEP during busy hours, this PEP can be applied to a live server and the reboot can be differed to a later time.

Note: Do not reboot the system until the PEP installation is finished, otherwise the PEP may not be properly registered on the server.

d). If anti-virus software was disabled, check to ensure it is now enabled. Note that it must be properly configured to scan "incoming" files only. See the bulletin on configuring anti-virus software for CallPilot.

6. Installation Log

File "SecPEP.log" in the root folder of the system drive will contain a log of the actions performed during PEP installation. In addition, a note will be added to the file "os_ver.txt", also in the root folder of the system drive.

7. PEP Uninstall

Due to the nature of the Microsoft hotfixes contained within this PEP, it cannot be uninstalled. Once applied, if removed from DMIViewer, only the references to PEP CPSECPEP009S in both DMIViewer and Windows Add/Remove Programs will be removed. Installation folder CPSECPEP009S under D:\TEMP will also be removed.

8. PEP Reinstallation

If required, this PEP may be installed again without any problem. Rerunning the PEP will reapply hotfixes and other configuration changes. If the PEP is not already in the PEP Utility (DMI Viewer), the PEP entry will be added when the PEP is reinstalled. If the PEP is already listed in the CallPilot PEP Utility (DMIViewer), it will not be added again to this utility.

9. Special installation instructions for Opsware:

No special instructions for installing this PEP via Opsware.

10. Supplemental Information - Verifying Hotfixes

To run the hot fix checker:
Double-click D:\TEMP\CPSECPEP009S\HotFixes\Checker\CheckHotFixes.bat

NOTE: The result (CheckResult.txt) will be opened in Notepad after the batch file execution; the result file contains two sections:

- Installed updates: list of all installed hotfixes.
- Missing Updates: list of missing hotfixes.