AVAYA

CallPilot Server Security Update - 2012

REVISION HISTORY

Date	Revision #	Summary of Changes
13 January 2012	Original bulletin	Publication in response to Microsoft security bulletins MS12-001 through MS12-007 on 10-Jan and 11-Jan.
13 January 2012	Rev. 1	Updated to refine support on MS11-100 and MS12-002.
16 February 2012	Rev. 2	Updated in response to Microsoft security bulletins MS12-008 through MS12-016 on 14-Feb and 15-Feb.
16 March 2012	Rev. 3	Updated in response to Microsoft security bulletins MS12-017 through MS12-022 on 13-Mar and 14-Mar.
13 April 2012	Rev. 4	Updated in response to Microsoft security bulletins MS12-023 through MS12-028 on 10-April.
11 May 2012	Rev. 5	Updated in response to Microsoft security bulletins MS12-029 through MS12-035 on 08-May and 09-May.
15 June 2012	Rev. 6	Updated in response to Microsoft security bulletins MS12-036 through MS12-042 on 12-Jun and 13-Jun; MS12-025 on 12-Jun and KB2718704 on 13-Jun.
13 July 2012	Rev. 7	Updated in response to Microsoft security bulletins MS12-043 through MS12-051 on 10-July.
17 August 2012	Rev. 8	Updated in response to Microsoft security bulletins MS12-052 through MS12-060 on 14-Aug and 15-Aug.
13 September 2012	Rev. 9	Updated in response to Microsoft security bulletins MS12-061 through MS12-062 on 11-Sep and 12-Sep.
12 October 2012	Rev. 10	Updated in response to Microsoft security bulletins MS12-063 on 21-Sep; and MS12-064 through MS12-070 on 09-Oct and 10-Oct.
16 Nov 2012	Rev. 11	Updated in response to Microsoft security bulletins MS12-071 through MS12-076 on 13-Nov and 14-Nov.

Introduction

This bulletin reflects the latest information regarding Microsoft security updates (hotfixes) for calendar year 2012 as they relate to Avaya CallPilot® software releases having life-cycle status of GA (Generally Available) or MD (End of Manufacturer Support) and their respective Windows Operating Systems. It also provides information on:

- Avaya's policy for testing security updates
- Notification timeframes for guidance on applying approved updates

- Details for using Microsoft's Windows Update utility
- CallPilot Security Update PEPs which contain Microsoft security updates and other CallPilot-specific security hardening enhancements
- Information on how to obtain CallPilot Security Update PEPs and Microsoft security updates

This document will be revised periodically in response to Microsoft security advisories to reflect the latest security information. It replaces product bulletins CallPilot Server Security Update-2011, P-2010-0001-Global, P-2009-0001-Global, P-2008-0008-Global, P-2007-0010-Global, P-2006-0011-Global, P-2005-0056-Global and P-2003-0277-Global.

Important Note: Effective December 31, 2006 Microsoft discontinued support for and no longer provides security updates for the Windows NT 4.0 Server OS. This affects the security vulnerability of CallPilot 2.5 and earlier systems. Avaya recommends these systems be upgraded to CallPilot 5.1 which is based on Windows Server 2003/Service Pack 2 (SP2)
and continues to receive critical OS updates from Microsoft which, if applied, ensure protection from OS-related vulnerabilities which could impact system performance and operation.

CallPilot Security Update PEPs

Avaya periodically provides comprehensive Server Security Update Product Enhancement Packages (PEPs) for use with CallPilot systems, generally with the introduction of a CallPilot Service Update (SU). Installation of these Security Update PEPs results in increased security of the CallPilot server. CallPilot Security Update PEPs are provided for convenience and offer the following benefits:

- Allows a large number of security updates to be applied easily, correctly, and quickly, usually with a single reboot.
- Are cumulative, containing all updates made available in earlier versions, so that only the most current version need be applied.
- Will not overwrite more recent security updates (if applied). For example, if the server is updated using Windows Update to a higher level than offered in a Security Update PEP, the PEP will not overwrite any more recent updates yet will apply all additional security improvements contained within.
- Applies non-Microsoft security updates as needed (e.g. pcAnywhere, Adobe Acrobat).
- Can be easily installed from CD so that a vulnerable system can be updated before exposing it to the network. This is particularly important when initially installing, or re-installing a CallPilot server.
- Performs other security hardening of the CallPilot server (e.g. disabling unused services, tighten folder permissions).

This bulletin outlines the recommended actions specific to these PEP updates, information on how to obtain each, and in Appendix-A, a detailed listing of each Microsoft Security Bulletin and its status as it pertains to CallPilot.

CallPilot Policy for Microsoft Security Updates (Hotfixes)

Background Information

- While most Microsoft security updates function properly on CallPilot, some security updates have been found to cause issues.
- CallPilot uses a particular combination and specific versions of various Microsoft Windows Operating System (OS), web server, and browser components. Therefore, Avaya does not install many security updates issued by Microsoft because only vulnerabilities in the components used by CallPilot need to be patched. CallPilot uses components in specific ways so the importance of a given vulnerability on CallPilot may differ from its importance when those components are used by non-CallPilot applications.
- Customers **should not** install non-Avaya-approved Microsoft security updates on the CallPilot server for the following reasons:
    - Customers may make mistakes in identifying which security updates are applicable to CallPilot and which exact version of a security update to apply.
    - Microsoft security updates must be tested to ensure they do not impact CallPilot functionality prior to being installed on customers' production servers.
    - If a customer alters the software or configuration of a CallPilot server in a manner not supported by Avaya, future upgrades of CallPilot software could fail even though the system presently works fine. Avaya testing is based on standard CallPilot configurations and cannot test all possible modifications of those configurations.

Important note: If a customer's IT/security requirements mandate that Microsoft security updates be applied within a timeframe prior to Avaya's communication, then they may be applied, but is done at their own risk. Support will remain available for the server, but if the security update is found to conflict with CallPilot, it will need to be removed which may require re-imaging the server and restoring from backup.

How Avaya Provides Microsoft Security Updates

- Each up-issue and release of CallPilot software incorporates the latest set of Microsoft security updates available at the time the release or up-issue was built. In addition to new security updates, each CallPilot software up-issue or release contains other security improvements that further harden CallPilot to attack.
- Each latest software release contains incremental security updates and enhancements over that of previous releases. Security-minded customers will therefore want to stay current with the latest release of CallPilot.
- When Microsoft issues a new security update, Avaya evaluates whether it applies to CallPilot, its threat-severity, and its impact on CallPilot operation and stability. After successful testing on software releases that are "GA", the security update is approved for direct download from Microsoft and installation on a CallPilot server.
    - Technical Security Advisory Bulletins are posted to https://support.avaya.com
    - Avaya will publish a response to each Microsoft Security Advisory Bulletin within three (3) business days of Microsoft notification, subject to availability of the update from Microsoft for the OS versions being tested and qualified. Responses will be in the form of a Technical Security Advisory Bulletin advising whether the new security update can be safely applied to CallPilot.

- All applicable Microsoft security updates will be made available via CallPilot "Server Security Update" PEPs that are released on a periodic basis for software releases with a "GA" Life-Cycle status. These "Server Security Update" PEPs provide a convenient installation package for Channel Partners to apply to CallPilot servers during scheduled maintenance windows, typically at the same time a CallPilot "Server Update" or SU is applied.

Important Note: Effective January 1, 2005, Microsoft discontinued support for use of Windows Update (http://windowsupdate.microsoft.com) for acquiring security updates for the Windows NT 4.0 Server OS. CallPilot NT 4.0-based systems are therefore no longer be able to utilize the Windows Update utility to obtain new security updates directly from Microsoft. In these cases, updates previously made available can be downloaded from the Enterprise Solution PEP Library (ESPL) website at: https://support.avaya.com/espl.

Recommended Actions

The following recommendations are provided to enhance security of the CallPilot server.

Change Windows Passwords to Strong Values

An important component of CallPilot server security is with passwords. Windows accounts with "weak" passwords are vulnerable to exploitation by currently active "worms" (e.g. LovGate). Following the recommended procedures documented within the NTPs, customers should ensure the passwords to the following Windows accounts are changed from their default values to new, strong values:

- Administrator
- NgenDesign
- NgenDist
- NgenSys
- gamroot (If present on RAID-equipped systems)

Apply Server Security Update PEPs and Microsoft Security Updates in concert

Complementary using the two update techniques reduces maintenance costs while providing improved security:

- Install the latest CallPilot Server Security Update PEPs when available during the next maintenance activity. These PEPs provide convenient, more complete server security updating.
- Install approved Microsoft security updates as needed for up-to-date Operating System (OS) specific fixes.

Failure to apply the updates could leave the system susceptible to one or more of the vulnerabilities causing system outage, or service degradation if exploited.

CallPilot Server Security Update PEPs may contain Microsoft security updates that have already been manually applied to the server in response to a published Technical Security Advisory bulletin, or Product Advisory Alert (PAA). In these scenarios, if one or more individual, approved security updates have been applied to the CallPilot server, they do not need to be removed prior to installing the CallPilot Server Security Update PEP. The Server Security Update PEP will overwrite any existing files during the installation process.

Remain Current

Because each software release contains security improvements, security-minded customers should upgrade to the current CallPilot release and apply the latest Security PEP to achieve the best protection.

Avoid any web-surfing from the CallPilot server

The CallPilot server includes a web-browser for performing administration tasks within CallPilot Manager. The browser should not be used for internet browsing. Doing so may introduce risk to the CallPilot server application and Operating System resulting in system outage or degradation of service.

Apply supplemental product updates where appropriate

- **Adobe Reader**

  On February 10, 2010, Adobe announced a security update for Adobe Reader for Windows. CallPilot 5.0 servers should be upgraded to Adobe Reader 9.3.3 to avoid this vulnerability.

  For additional details and installation procedures, reference bulletin PAA-2010-0006-Global / *CallPilot Security Update – Adobe Reader.*

- **Symantec pcAnywhere**

  On January 30, 2012, Symantec announced a security update for pcAnywhere. CallPilot 5.0/5.1 servers specifically utilize version 12.0 as outlined in the bulletin. pcAnywhere should be disabled, software removed from the server if alternate remote-control applications are being utilized, or have the update applied to avoid this vulnerability.

  For additional details and installation procedures for the Symantec pcAnywhere security update, reference bulletin *CallPilot Security Update – Symantec pcAnywhere.*

Server Security Update PEPs

The PEPs are cumulative updates including all Microsoft security updates and additional security hardening provided in earlier versions. For additional details, reference Appendix-A and Appendix-B. Only the most current version Server Security Update PEP is needed.

The PEPs are self-extracting executables that extract to a folder under D:\TEMP. (We do not recommend changing this folder.) Begin installation by copying the PEP to the server in the D:\TEMP folder, navigate to the D:\TEMP folder and execute the PEP to extract the files, then from the D:\TEMP\<PEP #> folder (e.g. D:\TEMP\CPSECPEP015S) review the readme.txt file for specific installation instructions.

PEP installation timeframes vary depending upon server processor speed, which update is being installed, and the number of updates being performed. Timeframes generally take between five (5) and fifty (50) minutes and may require multiple reboots.

The CallPilot Server Security Update PEPs are as follows:

CallPilot Release	Build	PEP number	Hotfix Level	File size	Notes
5.1	05.01	CPSECPEP015S	MS12-062	242MB	See note 3
5.0	05.00.04.20	CPSECPEP014S	MS11-034	174MB	
		CPSECPEPSP2S_v02	Service Pack 2	396MB	See note 3
		CPSECPEP013S	MS10-042	157MB	Obsolete
		CPSECPEP012S	MS09-065	142MB	Obsolete
		CPSECPEP011S	MS09-001	155MB	Obsolete
		CPSECPEP010S_v02	MS08-010	135MB	Obsolete
		CPSECPEP010S	MS08-010	163MB	Obsolete
		CPSECPEP009S	MS07-062	146MB	Obsolete
		CPSECPEP008S	MS07-054	124MB	Obsolete
		CPSECPEP007S	MS07-035	118MB	Obsolete
		CPSECPEP006S	MS07-022	105MB	Obsolete
4.0	04.04.04.00	CPSECPEP014S	MS11-034	174MB	
		CPSECPEPSP2S_v02	Service Pack 2	396MB	See note 3
		CPSECPEP013S	MS10-042	157MB	Obsolete
		CPSECPEP012S	MS09-065	142MB	Obsolete
		CPSECPEP011S	MS09-001	155MB	Obsolete
		CPSECPEP010S_v02	MS08-010	135MB	Obsolete
		CPSECPEP010S	MS08-010	163MB	Obsolete
		CPSECPEP009S	MS07-062	146MB	Obsolete
		CPSECPEP008S	MS07-054	118MB	Obsolete
		CPSECPEP007S	MS07-035	118MB	Obsolete
		CPSECPEP006S	MS07-022	105MB	Obsolete
		CP404SEC005S	MS06-065	84.0MB	Obsolete
		CP404SEC004S	MS06-016	51.5MB	Obsolete
		CP404SEC003S	MS05-053	31.3MB	Obsolete
3.0	03.03.06.02	CPSECPEP014S	MS11-034	174MB	See Notes 1-3
		CPSECPEPSP2S_v02	Service Pack 2	396MB	See note 3
		CP303SECSP1S	Service Pack 1	329MB	
		CPSECPEP013S	MS10-042	157MB	Obsolete

CallPilot Release	Build	PEP number	Hotfix Level	File size	Notes
3.0	03.03.06.02	CPSECPEP012S	MS09-065	142MB	Obsolete
		CPSECPEP011S	MS09-001	155MB	Obsolete
		CPSECPEP010S_v02	MS08-010	135MB	Obsolete
		CPSECPEP010S	MS08-010	163MB	Obsolete
		CPSECPEP009S	MS07-062	146MB	Obsolete
		CPSECPEP008S	MS07-054	118MB	Obsolete
		CPSECPEP007S	MS07-035	118MB	Obsolete
		CPSECPEP006S	MS07-022	105MB	Obsolete
		CP303SEC005S	MS06-065	89.5MB	Obsolete
		CP303SEC003S	MS05-053	36.9MB	Obsolete
		CP300SEC002S	MS05-015	57.7MB	Obsolete
2.5	2.50.06.14	CP250SEC003S	MS05-053	67.3MB	
		CP250SEC002S	MS05-015	60.3MB	Obsolete
		CP25006G082S	MS04-025	42.0MB	Obsolete
		CP25006G058S	MS04-007	13.4MB	Obsolete
		CP25006G014S	MS03-044	19.6MB	Obsolete
2.02	2.01.27.05	CP202SEC004S	MS06-025	76.8MB	
		CP202SEC003S	MS05-053	67.3MB	Obsolete
		CP202SEC002S	MS05-015	60.8MB	Obsolete
		CP202SEC001S	MS04-025	49.8MB	Obsolete
		CP20127G070S	MS04-007	13.4MB	Obsolete
		CP20127G050S	MS03-044	30.3MB	Obsolete
		CP20127G046S	MS03-024, 026, and MS03-039	27.5MB	Obsolete
		CP20127G039S	MS03-026	25.5MB	Obsolete

Notes:

1. This PEP requires PEP CP303SECSP1S (Windows Server 2003/Service Pack 1) be installed prior to installation.

2. Effective 10-April-2007, Microsoft no longer provides hotfix updates for non-SP1 systems. It's recommended to apply CP303SECSP1S and CPSECPEP010S_v02 to ensure any Microsoft updates made available after this date can be applied.

3. It's recommended all CallPilot 3.0, 4.0, 5.0, and 5.1 systems (excluding 202i IPE and 1006r Rackmount which include SP2 in the factory image) be updated to Windows Server 2003/Service Pack 2 (SP2). SP2 can be installed via PEP CPSECPEPSP2S_v02. See Appendix-E for details.

Obtaining the PEPs or older Microsoft Security Updates

CallPilot "Server Security Update" PEPs, as with all CallPilot PEPs, are available for download from the Enterprise Solutions PEP Library (ESPL) website at: https://support.avaya.com/espl.

Microsoft Security Updates for NT 4.0-based systems (2.02 and 2.5) are also available from this website.

Note: If you are new to the ESPL website, you will need to register for a user ID/password using the provided links for new user registration. Please apply on-line or contact your Avaya Channel Partner Account Manager.

References and Related Documents

For additional information on the installation of PEPs or operation of the PEP maintenance utility (DMI viewer), refer to the following documents:

CallPilot 5.1

- NTP NN44200-600 : Software Administration and Maintenance
- CallPilot 5.1 - Distributor Technical Reference

CallPilot 5.0

- NTP NN44200-600 : Software Administration and Maintenance
- Distributor Technical Reference (DTR) Bulletin: DTR-2007-0069-Global, CallPilot 5.0

CallPilot 4.0

- NTP 555-7101-202: Software Administration and Maintenance
- Distributor Technical Reference (DTR) Bulletin: DTR-2005-0226-Global, CallPilot 4.0

CallPilot 3.0 (Meridian 1 and CS 1000 only):

- NTP 555-7101-202: Software Administration and Maintenance
- Distributor Technical Reference (DTR) Bulletin: DTR-2004-0462-Global, CallPilot 3.0

CallPilot 2.5 (MSL-100 and DMS-100 only):

- NTP 555-7101-202: Installation & Configuration, Part 4: Software Installation and Maintenance
- General Release Bulletin: GR-2003-0417-Global, CallPilot 2.5

CallPilot 2.0 and 2.02 (Meridian 1 and CS 1000 only):

- NTP 555-7101-202: Installation & Configuration, Part 4: Software Installation and Maintenance
- General Release Bulletin: GR-2002-1582-Global, CallPilot 2.0
- General Release Bulletin: GR-2003-0191-Global, CallPilot 2.02

All documents are available for download from the Avaya Support Portal website at: https://support.avaya.com

Appendix-A

The following tables outline specific Microsoft Security Bulletins and associated security updates that pertain to the Windows Server 2003 (CallPilot 3.0, 4.0, 5.0, and 5.1) Operating System (OS) and associated Microsoft components. For each Microsoft security bulletin listed, it identifies whether or not it is applicable to CallPilot and if so, the corresponding release, PEP, or Security Update PEP required for addressing the vulnerability.

Note: CallPilot releases 2.5 and earlier which utilized the Windows NT 4.0 Server OS are End of Manufacturer Support and are **no longer tested or evaluated** against new Microsoft Security vulnerabilities. As well, Microsoft no longer provides any guidance or updates for Windows NT 4.0 Server. Security conscious customers are recommended to upgrade to CallPilot 5.1.

Note: Only those Microsoft security updates that have been approved for use with CallPilot or available via CallPilot PEPs or Service Updates should be applied to a CallPilot server. No other Microsoft security updates should ever be installed.

Legend:
SECnnS - Server Security PEP number which includes/implements the security update
GnnS - Server PEP number which includes/implement the security update
Sunn - Service Update required prior to implementing the security update
N/A - The security update is Not Applicable to CallPilot and therefore is not required nor installed
√ - The security update is incorporated into the base software release and no PEP/update is needed

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS12-076	11/13/12		Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2720184)	No Longer Evaluated		Not Applicable		
MS12-075	11/13/12	KB2761226	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2761226)	No Longer Evaluated		Approved	Approved	Approved
MS12-074	11/14/12	KB2698032 HA only: KB2729450	Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2745030) **Notes**: (26980322 – All), (2729450 for High Availability 1005r/1006r only) (Replaces multiple prior updates)	No Longer Evaluated		Approved (See Note)	Approved (See Note)	Approved (See Note)
MS12-073	11/14/12		Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Information Disclosure (2733829)	No Longer Evaluated		Not Applicable		
MS12-072	11/14/12	KB2727528	Vulnerabilities in Windows Shell Could Allow Remote Code Execution (2727528)	No Longer Evaluated		Approved	Approved	Approved

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS12-071	11/13/12		Cumulative Security Update for Internet Explorer (2761451)	No Longer Evaluated		Not Applicable		
MS12-070	10/09/12		Vulnerability in SQL Server Could Allow Elevation of Privilege (2754849)	No Longer Evaluated		Not Applicable		
MS12-069	10/09/12		Vulnerability in Kerberos Could Allow Denial of Service (2743555)	No Longer Evaluated		Not Applicable		
MS12-068	10/09/12	KB2724197	Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2724197) (Replaces MS12-042)	No Longer Evaluated		Approved	Approved	Approved
MS12-067	10/09/12		Vulnerabilities in FAST Search Server 2010 for SharePoint Parsing Could Allow Remote Code Execution (2742321)	No Longer Evaluated		Not Applicable		
MS12-066	10/10/12		Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)	No Longer Evaluated		Not Applicable		
MS12-065	10/09/12		Vulnerability in Microsoft Works Could Allow Remote Code Execution (2754670)	No Longer Evaluated		Not Applicable		
MS12-064	10/09/12		Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2742319)	No Longer Evaluated		Not Applicable		
MS12-063	09/21/12	KB2744842	Cumulative Security Update for Internet Explorer (2744842) (Replaces MS12-052)	No Longer Evaluated		Approved	Approved	Approved
MS12-062	09/12/12		Vulnerability in System Center Configuration Manager Could Allow Elevation of Privilege (2741528)	No Longer Evaluated		Not Applicable		
MS12-061	09/11/12		Vulnerability in Visual Studio Team Foundation Server Could Allow Elevation of Privilege (2719584)	No Longer Evaluated		Not Applicable		
MS12-060	08/14/12		Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2720573)	No Longer Evaluated		Not Applicable		
MS12-059	08/14/12		Vulnerability in Microsoft Visio Could Allow Remote Code Execution (2733918)	No Longer Evaluated		Not Applicable		
MS12-058	08/14/12		Vulnerabilities in Microsoft Exchange Server WebReady Document Viewing Could Allow Remote Code Execution (2740358)	No Longer Evaluated		Not Applicable		
MS12-057	08/14/12		Vulnerability in Microsoft Office Could Allow Remote Code Execution (2731879)	No Longer Evaluated		Not Applicable		
MS12-056	08/12/12		Vulnerability in JScript and VBScript Engines Could Allow Remote Code Execution (2706045)	No Longer Evaluated		Not Applicable		
MS12-055	08/14/12	KB2731847	Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2731847) (Replaces MS12-047)	No Longer Evaluated		Approved	Approved	Approved
MS12-054	08/15/12	KB2705219 KB2712808	Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594, 2705219, 2712808) (Replaces MS08-067 and MS09-022)	No Longer Evaluated		Approved	Approved	Approved

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS12-053	08/14/12		Vulnerability in Remote Desktop Could Allow Remote Code Execution (2723135)	No Longer Evaluated		Not Applicable		
MS12-052	08/15/12	KB2722913	Cumulative Security Update for Internet Explorer (2722913) (Replaces MS12-037)	No Longer Evaluated		Approved Superseded by MS12-063	Approved	Approved
MS12-051	07/10/12		Vulnerability in Microsoft Office for Mac Could Allow Elevation of Privilege (2721015)	No Longer Evaluated		Not Applicable		
MS12-050	07/10/12		Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	No Longer Evaluated		Not Applicable		
MS12-049	07/10/12	KB2655992	Vulnerability in TLS Could Allow Information Disclosure (2655992) (Replaces MS12-006)	No Longer Evaluated		Approved	Approved	Approved
MS12-048	07/10/12	KB2691442	Vulnerability in Windows Shell Could Allow Remote Code Execution (2691442) (Replaces MS10-046)	No Longer Evaluated		Approved	Approved	Approved
MS12-047	07/10/12	KB2718523	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2718523) (Replaces MS12-041)	No Longer Evaluated		Approved	Approved	Approved
MS12-046	07/10/12		Vulnerability in Visual Basic for Applications Could Allow Remote Code Execution (2707960)	No Longer Evaluated		Not Applicable		
MS12-045	07/10/12	KB2698365	Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (2698365)	No Longer Evaluated		Approved	Approved	Approved
MS12-044	07/10/12		Cumulative Security Update for Internet Explorer (2719177)	No Longer Evaluated		Not Applicable		
MS12-043	07/10/12	KB2719985 KB2721691 KB2721693	Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479, 2719985, 2721691, and 2721693) (Replaces MS10-051 and MS08-069)	No Longer Evaluated		Approved	Approved	Approved
MS12-042	06/12/12	KB2707511	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2711167, 2705711) (Replaces MS11-098)	No Longer Evaluated		Approved Superseded by MS12-068	Approved	Approved
MS12-041	06/12/12	KB2709162	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2709162) (Replaces MS12-018)	No Longer Evaluated		Approved	Approved	Approved
MS12-040	06/12/12		Vulnerability in Microsoft Dynamics AX Enterprise Portal Could Allow Elevation of Privilege (2709100)	No Longer Evaluated		Not Applicable		
MS12-039	06/12/12		Vulnerabilities in Lync Could Allow Remote Code Execution (2707956)	No Longer Evaluated		Not Applicable		
MS12-038	06/12/12	KB2686828	Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726, KB2686828) **Note**: (2686828 for High Availability 1005r/1006r only)	No Longer Evaluated		Approved (See Note)	Approved (See Note)	Approved (See Note)

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS12-037	06/12/12	KB2699988	Cumulative Security Update for Internet Explorer (2699988) (Replaces MS12-023)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS12-052		
MS12-036	06/13/12	KB2685939	Vulnerability in Remote Desktop Could Allow Remote Code Execution (2685939) Replaces MS11-065 and MS12-020)	No Longer Evaluated		Approved	Approved	Approved
	06/13/12	KB2718704	Unauthorized Digital Certificates Could Allow Spoofing (2718704)	No Longer Evaluated		Approved	Approved	Approved
MS12-035	05/08/12	KB2604078 HA only: KB2604092	Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777) **Notes**: (2604078 – All), (2604092 for High Availability 1005r/1006r only) (Replaces multiple prior updates)	No Longer Evaluated		Approved (See Note)	Approved (See Note)	Approved (See Note)
MS12-034	05/08/12	KB2659262, KB2676562, KB2686509	Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578) (2659262, 2676562, 2686509)	No Longer Evaluated		Approved	Approved	Approved
MS12-033	05/08/12		Vulnerability in Windows Partition Manager Could Allow Elevation of Privilege (2690533)	No Longer Evaluated		Not Applicable		
MS12-032	05/09/12		Vulnerability in TCP/IP Could Allow Elevation of Privilege (2688338)	No Longer Evaluated		Not Applicable		
MS12-031	05/08/12		Vulnerability in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2597981)	No Longer Evaluated		Not Applicable		
MS12-030	05/09/12		Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2663830)	No Longer Evaluated		Not Applicable		
MS12-029	05/09/12		Vulnerability in Microsoft Word Could Allow Remote Code Execution (2680352)	No Longer Evaluated		Not Applicable		
MS12-028	04/25/12		Vulnerability in Microsoft Office Could Allow Remote Code Execution (2639185)	No Longer Evaluated		Not Applicable		
MS12-027	04/10/12		Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2664258)	No Longer Evaluated		Not Applicable		
MS12-026	04/10/12		Vulnerabilities in Forefront Unified Access Gateway (UAG) Could Allow Information Disclosure	No Longer Evaluated		Not Applicable		
MS12-025	06/12/12	KB2656376 HA only: KB2656369	Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605) **Notes**: (2656376 – All), (2656369 for High Availability 1005r/1006r only)	No Longer Evaluated		Approved	Approved	Approved (See Note)
MS12-024	04/10/12	KB2653956	Vulnerability in Windows Could Allow Remote Code Execution (2653956) (Replaces MS10-019)	No Longer Evaluated		Approved	Approved	Approved
MS12-023	04/10/12	KB2675157	Cumulative Security Update for Internet Explorer (2675157) (Replaces MS12-010)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS12-037		
MS12-022	03/14/12		Vulnerability in Expression Design Could Allow Remote Code Execution (2651018)	No Longer Evaluated		Not Applicable		

<table>
<tr><th colspan="4">Microsoft Security Update Details</th><th colspan="5">CallPilot Release</th></tr>
<tr><th>Bulletin #</th><th>Date</th><th>Hotfix</th><th>Description</th><th>2.02</th><th>2.5</th><th>3.0</th><th>4.0</th><th>5.0/5.1</th></tr>
<tr><td>MS12-021</td><td>03/13/12</td><td></td><td>Vulnerability in Visual Studio Could Allow Elevation of Privilege (2651019)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td rowspan="2">MS12-020</td><td rowspan="2">03/13/12</td><td rowspan="2">KB2621440</td><td rowspan="2">Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (KB2570222 in MS11-065 replaced by KB2621440)</td><td colspan="2" rowspan="2">No Longer Evaluated</td><td>Approved</td><td>Approved</td><td>Approved</td></tr>
<tr><td colspan="3">Superseded by MS12-036</td></tr>
<tr><td>MS12-019</td><td>03/13/12</td><td></td><td>Vulnerability in DirectWrite Could Allow Denial of Service (2665364)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td rowspan="2">MS12-018</td><td rowspan="2">03/13/12</td><td rowspan="2">KB2641653</td><td rowspan="2">Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2641653) (Replaces MS12-008)</td><td colspan="2" rowspan="2">No Longer Evaluated</td><td>Approved</td><td>Approved</td><td>Approved</td></tr>
<tr><td colspan="3">Superseded by MS12-041</td></tr>
<tr><td>MS12-017</td><td>03/13/12</td><td></td><td>Vulnerability in DNS Server Could Allow Denial of Service (2647170) (Replaces MS11-058)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td rowspan="2">MS12-016</td><td rowspan="2">02/15/12</td><td rowspan="2">KB2633880</td><td rowspan="2">Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026) (2633880) (Replaces MS11-069)</td><td colspan="2" rowspan="2">No Longer Evaluated</td><td colspan="2">Not Applicable</td><td>Approved for H/A systems</td></tr>
<tr><td colspan="3">Superseded by MS12-035 and MS12-074</td></tr>
<tr><td>MS12-015</td><td>02/14/12</td><td></td><td>Vulnerabilities in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2663510)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td>MS12-014</td><td>02/14/12</td><td></td><td>Vulnerability in Indeo Codec Could Allow Remote Code Execution (2661637)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td>MS12-013</td><td>02/14/12</td><td></td><td>Vulnerability in C Run-Time Library Could Allow Remote Code Execution (2654428)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td>MS12-012</td><td>02/14/12</td><td></td><td>Vulnerability in Color Control Panel Could Allow Remote Code Execution (2643719)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td>MS12-011</td><td>02/14/12</td><td></td><td>Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td rowspan="2">MS12-010</td><td rowspan="2">02/14/12</td><td rowspan="2">KB2647516</td><td rowspan="2">Cumulative Security Update for Internet Explorer (2647516) (Replaces MS11-099</td><td colspan="2" rowspan="2">No Longer Evaluated</td><td>Approved</td><td>Approved</td><td>Approved</td></tr>
<tr><td colspan="3">Superseded by MS12-023</td></tr>
<tr><td>MS12-009</td><td>02/14/12</td><td>KB2645640</td><td>Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640) (Replaces MS11-080)</td><td colspan="2">No Longer Evaluated</td><td>Approved</td><td>Approved</td><td>Approved</td></tr>
<tr><td rowspan="2">MS12-008</td><td rowspan="2">02/14/12</td><td rowspan="2">KB2660465</td><td rowspan="2">Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465) (Replaces MS11-087)</td><td colspan="2" rowspan="2">No Longer Evaluated</td><td>Approved</td><td>Approved</td><td>Approved</td></tr>
<tr><td colspan="3">Superseded by MS12-018</td></tr>
<tr><td>MS12-007</td><td>01/11/12</td><td></td><td>Vulnerability in AntiXSS Library Could Allow Information Disclosure (2607664)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td rowspan="2">MS12-006</td><td rowspan="2">01/10/12</td><td rowspan="2">KB2585542
KB2638806</td><td rowspan="2">Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584) (2585542 and 2638806) (Replaces MS10-049)</td><td colspan="2" rowspan="2">No Longer Evaluated</td><td>Approved</td><td>Approved</td><td>Approved</td></tr>
<tr><td colspan="3">Superseded by MS12-049</td></tr>
<tr><td>MS12-005</td><td>01/10/12</td><td>KB2584146</td><td>Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146)</td><td colspan="2">No Longer Evaluated</td><td>Approved</td><td>Approved</td><td>Approved</td></tr>
</table>

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS12-004	01/11/12	KB2598479 KB2631813	Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391) (2598479 and 2631813) (Replaces MS10-033)	No Longer Evaluated		Approved	Approved	Approved
MS12-003	01/10/12	KB2646524	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2646524) (Replaces MS11-063)	No Longer Evaluated		Approved	Approved	Approved
MS12-002	01/10/12	KB2603381	Vulnerability in Windows Object Packager Could Allow Remote Code Execution (2603381)	No Longer Evaluated		Approved	Approved	Approved
MS12-001	01/10/12	KB2644615	Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615)	No Longer Evaluated		Approved	Approved	Approved
MS11-100	12/30/11	KB2656358 H/A only: KB2656352 KB2657424	Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (Replaces MS10-070) **Notes**: (2656358 - All), (2656352 and 2657424 for High Availability 1005r/1006r only)	No Longer Evaluated		Approved (See Note)	Approved (See Note)	Approved (See Note)
MS11-099	12/13/11	KB2618444	Cumulative Security Update for Internet Explorer (2618444) (Replaces MS11-081)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS12-010		
MS11-098	12/13/11	KB2633171	Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2633171) (Replaces MS10-021)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS12-042		
MS11-097	12/13/11	KB2620712	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2620712) (Replaces MS11-010)	No Longer Evaluated		Approved	Approved	Approved
MS11-096	12/13/11		Vulnerability in Microsoft Excel Could Allow Remote Code Execution (2640241)	No Longer Evaluated		Not Applicable		
MS11-095	12/13/11		Vulnerability in Active Directory Could Allow Remote Code Execution (2640045)	No Longer Evaluated		Not Applicable		
MS11-094	12/13/11		Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2639142)	No Longer Evaluated		Not Applicable		
MS11-093	12/13/11	KB2624667	Vulnerability in OLE Could Allow Remote Code Execution (2624667)	No Longer Evaluated		Approved	Approved	Approved
MS11-092	12/13/11		Vulnerability in Windows Media Could Allow Remote Code Execution (2648048)	No Longer Evaluated		Not Applicable		
MS11-091	12/13/11		Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2607702)	No Longer Evaluated		Not Applicable		
MS11-090	12/13/11	KB2618451	Cumulative Security Update of ActiveX Kill Bits (2618451) (Replaces MS11-027)	No Longer Evaluated		Approved	Approved	Approved
MS11-089	12/13/11		Vulnerability in Microsoft Office Could Allow Remote Code Execution (2590602)	No Longer Evaluated		Not Applicable		
MS11-088	12/14/11		Vulnerability in Microsoft Office IME (Chinese) Could Allow Elevation of Privilege (2652016)	No Longer Evaluated		Not Applicable		
MS11-087	12/13/11	KB2639417	Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417) (Replaces MS11-077)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS12-008		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS11-086	11/08/11		Vulnerability in Active Directory Could Allow Elevation of Privilege (2630837)	No Longer Evaluated		Not Applicable		
MS11-085	11/08/11		Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution (2620704)	No Longer Evaluated		Not Applicable		
MS11-084	11/08/11		Vulnerability in Windows Kernel-Mode Drivers Could Allow Denial of Service (2617657)	No Longer Evaluated		Not Applicable		
MS11-083	11/08/11		Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516)	No Longer Evaluated		Not Applicable		
MS11-082	10/11/11		Vulnerabilities in Host Integration Server Could Allow Denial of Service (2607670)	No Longer Evaluated		Not Applicable		
MS11-081	10/12/11	KB2586448	Cumulative Security Update for Internet Explorer (2586448) (Replaces MS11-057)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-099		
MS11-080	10/11/11	KB2592799	Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2592799) (Replaces MS11-046)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS12-009		
MS11-079	10/11/11		Vulnerabilities in Microsoft Forefront Unified Access Gateway Could Cause Remote Code Execution (2544641)	No Longer Evaluated		Not Applicable		
MS11-078	10/11/11	KB2572069	Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (20572069) (2604930) (Replaces MS09-061)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS12-035 and MS12-074		
MS11-077	10/11/11	KB2567053	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2567053) (Replaces MS11-054)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-087		
MS11-076	10/11/11		Vulnerability in Windows Media Center Could Allow Remote Code Execution (2604926)	No Longer Evaluated		Not Applicable		
MS11-075	10/12/11	KB2564958	Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution (2623699) (KB2564958)	No Longer Evaluated		Approved	Approved	Approved
MS11-074	09/13/11		Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	No Longer Evaluated		Not Applicable		
MS11-073	09/13/11		Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2587634)	No Longer Evaluated		Not Applicable		
MS11-072	09/13/11		Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2587505)	No Longer Evaluated		Not Applicable		
MS11-071	09/13/11	KB2570947	Vulnerability in Windows Components Could Allow Remote Code Execution (2570947)	No Longer Evaluated		Approved	Approved	Approved
MS11-070	09/13/11		Vulnerability in WINS Could Allow Elevation of Privilege (2571621) (Replaces MS11-035)	No Longer Evaluated		Not Applicable		
MS11-069	08/09/11		Vulnerability in .NET Framework Could Allow Information Disclosure (2567951)	No Longer Evaluated		Not Applicable		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS11-068	08/10/11		Vulnerability in Windows Kernel Could Allow Denial of Service (2556532)	No Longer Evaluated		Not Applicable		
MS11-067	08/09/11		Vulnerability in Microsoft Report Viewer Could Allow Information Disclosure (2578230)	No Longer Evaluated		Not Applicable		
MS11-066	08/09/11		Vulnerability in Microsoft Chart Control Could Allow Information Disclosure (2567943)	No Longer Evaluated		Not Applicable		
MS11-065	08/09/11	KB2570222	Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (2570222)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS12-036		
MS11-064	08/09/11		Vulnerabilities in TCP/IP Stack Could Allow Denial of Service (2563894)	No Longer Evaluated		Not Applicable		
MS11-063	08/09/11	KB2567680	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2567680) (Replaces MS10-069)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS12-003		
MS11-062	08/09/11	KB2566454	Vulnerability in Remote Access Service NDISTAPI Driver Could Allow Elevation of Privilege (2566454)	No Longer Evaluated		Approved	Approved	Approved
MS11-061	08/09/11		Vulnerability in Remote Desktop Web Access Could Allow Elevation of Privilege (2546250)	No Longer Evaluated		Not Applicable		
MS11-060	08/09/11		Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (2560978)	No Longer Evaluated		Not Applicable		
MS11-059	08/10/11		Vulnerability in Data Access Components Could Allow Remote Code Execution (2560656)	No Longer Evaluated		Not Applicable		
MS11-058	08/09/11		Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (Replaces MS09-008, MS09-048, and MS11-046)	No Longer Evaluated		Not Applicable		
MS11-057	08/09/11	KB2559049	Cumulative Security Update for Internet Explorer (2559049) (Replaces MS11-050)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-081		
MS11-056	07/12/11	KB2507938	Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2507938) (Replaces MS11-10 and MS10-069)	No Longer Evaluated		Approved	Approved	Approved
MS11-055	07/12/11		Vulnerability in Microsoft Visio Could Allow Remote Code Execution (2560847)	No Longer Evaluated		Not Applicable		
MS11-054	07/12/11	KB2555917	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917) (Replaces MS11-034)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-077		
MS11-053	07/12/11		Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (2566220)	No Longer Evaluated		Not Applicable		
MS11-052	06/14/11	KB2544521	Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2544521)	No Longer Evaluated		Approved	Approved	Approved

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS11-051	06/15/11		Vulnerability in Active Directory Certificate Services Web Enrollment Could Allow Elevation of Privilege (2518295)	No Longer Evaluated		Not Applicable		
MS11-050	06/14/11	KB2530548	Cumulative Security Update for Internet Explorer (2530548) (Replaces MS11-018)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-057		
MS11-049	06/15/11		Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure (2543893)	No Longer Evaluated		Not Applicable		
MS11-048	06/14/11		Vulnerability in SMB Server Could Allow Denial of Service (2536275)	No Longer Evaluated		Not Applicable		
MS11-047	06/14/11		Vulnerability in Hyper-V Could Allow Denial of Service (2525835)	No Longer Evaluated		Not Applicable		
MS11-046	06/14/11	KB2503665	Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2503665)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-058		
MS11-045	06/14/11		Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2537146)	No Longer Evaluated		Not Applicable		
MS11-044	06/14/11		Vulnerability in .NET Framework Could Allow Remote Code Execution (2538814)	No Longer Evaluated		Not Applicable		
MS11-043	06/14/11	KB2536276	Vulnerability in SMB Client Could Allow Remote Code Execution (2536276) (Replaces MS11-019)	No Longer Evaluated		Approved	Approved	Approved
MS11-042	06/14/11	KB2535512	Vulnerabilities in Distributed File System Could Allow Remote Code Execution (2535512)	No Longer Evaluated		Approved	Approved	Approved
MS11-041	06/14/11		Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2525694)	No Longer Evaluated		Not Applicable		
MS11-040	06/14/11		Vulnerability in Threat Management Gateway Firewall Client Could Allow Remote Code Execution (2520426)	No Longer Evaluated		Not Applicable		
MS11-039	06/14/11		Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2514842)	No Longer Evaluated		Not Applicable		
MS11-038	06/14/11		Vulnerability in OLE Automation Could Allow Remote Code Execution (2476490) (Replaces MS08-008)	No Longer Evaluated		Approved	Approved	Approved
MS11-037	11/08/11		Vulnerability in MHTML Could Allow Information Disclosure (2544893) (Replaces MS11-026)	No Longer Evaluated		Approved	Approved	Approved
MS11-036	06/14/11		Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2545814)	No Longer Evaluated		Not Applicable		
MS11-035	05/10/11	KB2524426	Vulnerability in WINS Could Allow Remote Code Execution (2524426) (Replaces MS09-039)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-070		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS11-034	04/12/11	KB2506223	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2506223) (Replaces MS11-012)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
						Superseded by MS11-054		
MS11-033	04/12/11	KB2485663	Vulnerability in WordPad Text Converters Could Allow Remote Code Execution (2485663) (Replaces MS10-067)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS11-032	04/12/11	KB2507618	Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2507618) (Replaces MS11-007)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS11-031	04/12/11		Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2514666) (Replaces MS09-045 and MS10-022)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS11-030	04/12/11	KB2509553	Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (Replaces MS08-020, MS08-037, and MS08-066)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS11-029	04/12/11	KB2412687	Vulnerability in GDI+ Could Allow Remote Code Execution (2489979) (Replaces MS09-062)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS11-028	04/12/11		Vulnerability in .NET Framework Could Allow Remote Code Execution (2484015) (Replaces MS09-061, MS10-060, and MS10-077)	No Longer Evaluated		Not Applicable		
MS11-027	04/12/11	KB2508272	Cumulative Security Update of ActiveX Kill Bits (2508272) (Replaces MS10-034)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
						Superseded by MS11-090		
MS11-026	04/12/11	KB2503658	Vulnerability in MHTML Could Allow Information Disclosure (2503658)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
						Superseded by MS11-037		
MS11-025	04/12/11		Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution (2500212)	No Longer Evaluated		Not Applicable		
MS11-024	04/12/11	KB2491683 KB2506212	Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution (2527308)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS11-023	04/12/11		Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2489293)	No Longer Evaluated		Not Applicable		
MS11-022	04/12/11		Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2489283)	No Longer Evaluated		Not Applicable		
MS11-021	04/12/11		Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2489279)	No Longer Evaluated		Not Applicable		
MS11-020	04/12/11	KB2508429	Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (Replaces MS10-054)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS11-019	04/13/11	KB2511455	Vulnerabilities in SMB Client Could Allow Remote Code Execution (2511455)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-043		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS11-018	04/12/11	KB2497640	Cumulative Security Update for Internet Explorer (2497640) (Replaces MS11-003)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
						Superseded by MS11-050		
MS11-017	03/08/11		Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (2508062)	No Longer Evaluated		Not Applicable		
MS11-016	03/08/11		Vulnerability in Microsoft Groove Could Allow Remote Code Execution (2494047)	No Longer Evaluated		Not Applicable		
MS11-015	03/08/11		Vulnerabilities in Windows Media Could Allow Remote Code Execution (2510030)	No Longer Evaluated		Not Applicable		
MS11-014	02/08/11	KB2478960	Vulnerability in Local Security Authority Subsystem Service Could Allow Local Elevation of Privilege (2478960) (Replaces MS08-002)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS11-013	02/08/11	KB2478971	Vulnerabilities in Kerberos Could Allow Elevation of Privilege (2496930) (2478971) (Replaces MS10-014)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS11-012	02/08/11	KB2479628	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628) (Replaces MS10-098)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-034		
MS11-011	02/08/11	KB2393802	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) (Replaces MS10-021)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS11-010	02/08/11	KB2476687	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2476687) (Replaces MS10-011)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
						Superseded by MS11-056		
MS11-009	02/08/11		Vulnerability in JScript and VBScript Scripting Engines Could Allow Information Disclosure (2475792)	No Longer Evaluated		Not Applicable		
MS11-008	02/08/11		Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (2451879)	No Longer Evaluated		Not Applicable		
MS11-007	02/08/11	KB2485376	Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2485376) (Replaces MS10-091)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-032		
MS11-006	02/08/11	KB2483185	Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185) (Replaces MS10-046)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS11-005	02/08/11		Vulnerability in Active Directory Could Allow Denial of Service (2478953)	No Longer Evaluated		Not Applicable		
MS11-004	02/08/11		Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256)	No Longer Evaluated		Not Applicable		
MS11-003	02/08/11	KB2482017	Cumulative Security Update for Internet Explorer (2482017) (Replaces MS10-090)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-018		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS11-002	01/11/11	KB2419635	Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution (2451910) (2419635)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS11-001	01/11/11		Vulnerability in Windows Backup Manager Could Allow Remote Code Execution (2478935)	No Longer Evaluated		Not Applicable		
MS10-106	12/14/10		Vulnerability in Microsoft Exchange Server Could Allow Denial of Service (2407132)	No Longer Evaluated		Not Applicable		
MS10-105	12/15/10		Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095)	No Longer Evaluated		Not Applicable		
MS10-104	12/14/10		Vulnerability in Microsoft SharePoint Could Allow Remote Code Execution (2455005)	No Longer Evaluated		Not Applicable		
MS10-103	12/14/10		Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2292970)	No Longer Evaluated		Not Applicable		
MS10-102	12/14/10		Vulnerability in Hyper-V Could Allow Denial of Service (2345316)	No Longer Evaluated		Not Applicable		
MS10-101	12/14/10	KB2207559	Vulnerability in Windows Netlogon Service Could Allow Denial of Service (2207559)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-100	12/14/10		Vulnerability in Consent User Interface Could Allow Elevation of Privilege (2442962)	No Longer Evaluated		Not Applicable		
MS10-099	12/14/10	KB2440591	Vulnerability in Routing and Remote Access Could Allow Elevation of Privilege (2440591)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-098	12/14/10	KB2436673	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673) (Replaces MS10-073)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-012		
MS10-097	12/14/10	KB2443105	Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution (2443105)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-096	12/14/10	KB2423089	Vulnerability in Windows Address Book Could Allow Remote Code Execution (2423089)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-095	12/14/10		Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2385678)	No Longer Evaluated		Not Applicable		
MS10-094	12/14/10		Vulnerability in Windows Media Encoder Could Allow Remote Code Execution (2447961) (Replaces MS08-053 and MS10-033)	No Longer Evaluated		Not Applicable		
MS10-093	12/14/10		Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (2424434)	No Longer Evaluated		Not Applicable		
MS10-092	12/14/10		Vulnerability in Task Scheduler Could Allow Elevation of Privilege (2305420)	No Longer Evaluated		Not Applicable		
MS10-091	12/14/10	KB2296199	Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution (2296199) (Replaces MS10-078)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-007		
MS10-090	12/14/10	KB2416400	Cumulative Security Update for Internet Explorer (2416400) (Replaces MS10-071)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-003		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS10-089	11/09/10		Vulnerabilities in Forefront Unified Access Gateway (UAG) Could Allow Elevation of Privilege (2316074)	No Longer Evaluated		Not Applicable		
MS10-088	11/09/10		Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2293386)	No Longer Evaluated		Not Applicable		
MS10-087	11/09/10		Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2423930)	No Longer Evaluated		Not Applicable		
MS10-086	10/12/10		Vulnerability in Windows Shared Cluster Disks Could Allow Tampering (2294255)	No Longer Evaluated		Not Applicable		
MS10-085	10/12/10		Vulnerability in SChannel Could Allow Denial of Service (2207566)	No Longer Evaluated		Not Applicable		
MS10-084	10/12/10	KB2360937	Vulnerability in Windows Local Procedure Call Could Cause Elevation of Privilege (2360937) (Replaces MS10-066)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-083	10/12/10	KB979687	Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution (2405882) (979687)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-082	10/13/10	KB2378111	Vulnerability in Windows Media Player Could Allow Remote Code Execution (2378111)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-081	10/12/10	KB2296011	Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2296011)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-080	10/12/10		Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	No Longer Evaluated		Not Applicable		
MS10-079	10/13/10		Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)	No Longer Evaluated		Not Applicable		
MS10-078	10/12/10	KB2279986	Vulnerabilities in the OpenType Font (OTF) Format Driver Could Allow Elevation of Privilege (2279986) (Replaces MS10-037)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS10-091		
MS10-077	10/13/10		Vulnerability in .NET Framework Could Allow Remote Code Execution (2160841)	No Longer Evaluated		Not Applicable		
MS10-076	10/12/10	KB982132	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (982132)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-075	10/12/10		Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution (2281679)	No Longer Evaluated		Not Applicable		
MS10-074	10/12/10	KB2387149	Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution (2387149) (Replaces MS07-012)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-073	10/12/10	KB981957	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) (Replaces MS10-048)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS10-098		
MS10-072	10/13/10		Vulnerabilities in SafeHTML Could Allow Information Disclosure (2412048)	No Longer Evaluated		Not Applicable		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS10-071	10/13/10	KB2360131	Cumulative Security Update for Internet Explorer (2360131) (Replaces MS10-053)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS10-090		
MS10-070	10/13/10	KB2416451	Vulnerability in ASP.NET Could Allow Information Disclosure (2418042)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
						Superseded by MS11-100		
MS10-069	09/14/10	KB2121546	Vulnerability in Windows Client/Server Runtime Subsystem Could Allow Elevation of Privilege (2121546) (Replaces MS07-021)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
						Superseded by MS11-056, then MS11-063		
MS10-068	09/14/10		Vulnerability in Local Security Authority Subsystem Service Could Allow Elevation of Privilege (983539) (Replaces MS09-066)	No Longer Evaluated		Not Applicable		
MS10-067	09/14/10	KB2259922	Vulnerability in WordPad Text Converters Could Allow Remote Code Execution (2259922)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-033		
MS10-066	09/14/10	KB982802	Vulnerability in Remote Procedure Call Could Allow Remote Code Execution (982802) (Replaces MS09-026)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS10-084		
MS10-065	09/14/10	KB2124261	Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2124261) (Replaces MS08-006)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-064	09/14/10		Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (2315011)	No Longer Evaluated		Not Applicable		
MS10-063	09/14/10	KB981322	Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (2320113) (981322)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-062	09/14/10	KB975558	Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution (975558)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-061	09/14/10	KB2347290	Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-060	08/11/10		Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (2265906)	No Longer Evaluated		Not Applicable		
MS10-059	08/10/10		Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799)	No Longer Evaluated		Not Applicable		
MS10-058	08/10/10		Vulnerabilities in TCP/IP Could Allow Elevation of Privilege (978886)	No Longer Evaluated		Not Applicable		
MS10-057	08/11/10		Vulnerability in Microsoft Office Excel Could Allow Remote Code Execution (2269707)	No Longer Evaluated		Not Applicable		
MS10-056	08/11/10		Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638)	No Longer Evaluated		Not Applicable		
MS10-055	08/12/10		Vulnerability in Cinepak Codec Could Allow Remote Code Execution (982665)	No Longer Evaluated		Not Applicable		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS10-054	08/11/10	KB982214	Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (Replaces MS10-012)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-020		
MS10-053	08/10/10	KB2183461	Cumulative Security Update for Internet Explorer (2183461) (Replaces MS10-035)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS10-071		
MS10-052	08/10/10	KB2115168	Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (2115168)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-051	08/10/10	KB2079403	Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2079403) (Replaces MS08-069)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
						Superseded by MS12-043		
MS10-050	08/11/10		Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (981997)	No Longer Evaluated		Not Applicable		
MS10-049	08/10/10	KB980436	Vulnerabilities in Schannel could allow Remote Code Execution (980436)	No Longer Evaluated		SEC014S	SEC014S	SEC014S
MS10-048	08/10/10	KB2160329	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329) (Replaces MS10-032)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS10-073		
MS10-047	08/10/10		Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)	No Longer Evaluated		Not Applicable		
MS10-046	08/03/10	KB2286198	Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS11-006		
MS10-045	07/14/10		Vulnerability in Microsoft Office Outlook Could Allow Remote Code Execution (978212)	No Longer Evaluated		Not Applicable		
MS10-044	07/14/10		Vulnerabilities in Microsoft Office Access ActiveX Controls Could Allow Remote Code Execution (982335)	No Longer Evaluated		Not Applicable		
MS10-043	07/14/10		Vulnerability in Canonical Display Driver Could Allow Remote Code Execution (2032276)	No Longer Evaluated		Not Applicable		
MS10-042	07/13/10	KB2229593	Vulnerability in Help and Support Center Could Allow Remote Code Execution (2229593)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS10-041	06/08/10	KB979907 KB979909	Vulnerability in Microsoft .NET Framework Could Allow Tampering (981343 and 979907) **Note**: 9799909 for High Availability 1005r/1006r only)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS10-040	06/08/10	KB982666	Vulnerability in Internet Information Services Could Allow Remote Code Execution (982666)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS10-039	06/08/10		Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2028554)	No Longer Evaluated		Not Applicable		
MS10-038	06/09/10		Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	No Longer Evaluated		Not Applicable		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS10-037	06/08/10	KB980218	Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege (980218)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
						Superseded by MS10-078		
MS10-036	06/08/10		Vulnerability in COM Validation in Microsoft Office Could Allow Remote Code Execution (983235)	No Longer Evaluated		Not Applicable		
MS10-035	06/08/10	KB982381	Cumulative Security Update for Internet Explorer (982381) (Replaces MS10-018)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
						Superseded by MS10-053		
MS10-034	06/08/10	KB980195	Cumulative Security Update of ActiveX Kill Bits (980195) (Replaces MS10-008)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
						IMPORTANT: See Note 7 Superseded by MS11-027		
MS10-033	06/09/10	KB975562 KB978695 KB979482	Vulnerabilities in Media Decompression Could Allow Remote Code Execution (975562, 978695, and 979482) (Replaces MS09-028 and MS09-047)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
						Superseded by MS12-004		
MS10-032	06/08/10	KB979559	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559) (Replaces MS09-065)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
						Superseded by MS10-048		
MS10-031	05/11/10		Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (978213)	No Longer Evaluated		Not Applicable		
MS10-030	05/12/10		Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution (978542)	No Longer Evaluated		Not Applicable		
MS10-029	04/13/10	KB978338	Vulnerability in Windows ISATAP Component Could Allow Spoofing (978338)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS10-028	04/13/10		Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (980094)	No Longer Evaluated		Not Applicable		
MS10-027	04/13/10		Vulnerability in Windows Media Player Could Allow Remote Code Execution (979402)	No Longer Evaluated		Not Applicable		
MS10-026	04/13/10	KB977816	Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (977816)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS10-025	04/13/10		Vulnerability in Microsoft Windows Media Services Could Allow Remote Code Execution (980858)	No Longer Evaluated		Not Applicable		
MS10-024	04/13/10		Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832)	No Longer Evaluated		Not Applicable		
MS10-023	04/13/10		Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (981160)	No Longer Evaluated		Not Applicable		
MS10-022	04/13/10	KB981350	Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981350)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
						Superseded by MS11-031		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS10-021	04/13/10	KB979683	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683) (Replaces MS10-015)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
						Superseded by MS11-011		
MS10-020	04/13/10	KB980232	Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232) (Replaces MS10-006)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS10-019	04/15/10	KB978601 KB979309	Vulnerabilities in Windows Could Allow Remote Code Execution (981210)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
						Superseded by MS12-024		
MS10-018	03/30/10	KB980182	Cumulative Security Update for Internet Explorer (980182). (Replaces MS10-002)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS10-035		
MS10-017	03/10/10		Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)	No Longer Evaluated		Not Applicable		
MS10-016	03/09/10		Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (975561)	No Longer Evaluated		Not Applicable		
MS10-015	02/10/10	KB977165	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165) (Replaces MS09-058)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS10-021		
MS10-014	02/09/10		Vulnerability in Kerberos Could Allow Denial of Service (977290)	No Longer Evaluated		Not Applicable		
MS10-013	02/10/10	KB977914 KB975560	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935) (Replaces MS09-028 and MS09-038)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS10-012	02/10/10	KB971468	Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468) (Replaces MS09-001)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
						Superseded by MS10-054		
MS10-011	02/10/10	KB978037	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (978037)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
						Superseded by MS11-010		
MS10-010	02/10/10		Vulnerability in Windows Server 2008 Hyper-V Could Allow Denial of Service (977894)	No Longer Evaluated		Not Applicable		
MS10-009	02/10/10		Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	No Longer Evaluated		Not Applicable		
MS10-008	02/10/10	KB978262	Cumulative Security Update of ActiveX Kill Bits (978262) (Replaces MS09-055)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS10-034		
MS10-007	02/09/10	KB975713	Vulnerability in Windows Shell Handler Could Allow Remote Code Execution (975713)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS10-006	02/10/10	KB978251	Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251) (Replaces MS08-068)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS10-020		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS10-005	02/10/10	KB978706	Vulnerability in Microsoft Paint Could Allow Remote Code Execution (978706)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS10-004	02/09/10		Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (975416)	No Longer Evaluated		Not Applicable		
MS10-003	02/10/10		Vulnerability in Microsoft Office (MSO) Could Allow Remote Code Execution (978214)	No Longer Evaluated		Not Applicable		
MS10-002	01/21/10	KB978207	Cumulative Security Update for Internet Explorer (978207) (Replaces MS09-072)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS10-018		
MS10-001	01/12/10	KB972270	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270) (Replaces MS09-029)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS09-074	12/08/09		Vulnerability in Microsoft Office Project Could Allow Remote Code Execution (967183)	No Longer Evaluated		Not Applicable		
MS09-073	12/09/09	KB973904	Vulnerability in WordPad and Office Text Converters Could Allow Remote Code Execution (975539) (973904)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS09-072	12/09/09	KB976325	Cumulative Security Update for Internet Explorer (976325) (Replaces MS09-054)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS10-002		
MS09-071	12/09/09	KB974318	Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS09-070	12/09/09		Vulnerabilities in Active Directory Federation Services Could Allow Remote Code Execution (971726)	No Longer Evaluated		Not Applicable		
MS09-069	12/08/09	KB974392	Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (974392)	No Longer Evaluated		SEC013S	SEC013S	SEC013S
MS09-068	11/10/09		Vulnerability in Microsoft Office Word Could Allow Remote Code Execution (976307)	No Longer Evaluated		Not Applicable		
MS09-067	11/10/09		Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (972652)	No Longer Evaluated		Not Applicable		
MS09-066	11/10/09		Vulnerability in Active Directory Could Allow Denial of Service (973309)	No Longer Evaluated		Not Applicable		
MS09-065	11/12/09	KB969947	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947) (Replaces MS09-025)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS10-032		
MS09-064	11/10/09		Vulnerability in License Logging Server Could Allow Remote Code Execution (974783)	No Longer Evaluated		Not Applicable		
MS09-063	11/10/09		Vulnerability in Web Services on Devices API Could Allow Remote Code Execution (973565)	No Longer Evaluated		Not Applicable		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS09-062	10/14/09	KB958869	Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488) (968869) (Replaces MS08-052)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS11-029		
MS09-061	10/13/09	KB953298 KB953300 KB974417	Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution (974378) (Replaces MS07-040)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS11-028		
MS09-060	10/13/09		Vulnerabilities in Microsoft Active Template Library (ATL) ActiveX Controls for Microsoft Office Could Allow Remote Code Execution (973965)	No Longer Evaluated		Not Applicable		
MS09-059	10/14/09	KB975467	Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (975467) (If KB968389 applied)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-058	10/13/09	KB971486	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (971486) (Replaces MS08-064)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS10-015		
MS09-057	10/13/09	KB969059	Vulnerability in Indexing Service Could Allow Remote Code Execution (969059)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-056	10/14/09	KB974571	Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-055	10/14/09	KB973525	Cumulative Security Update of ActiveX Kill Bits (973525) (Replaces MS09-032)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS10-008		
MS09-054	10/13/09	KB974455	Cumulative Security Update for Internet Explorer (974455) (Replaces MS09-034) (Recommend also apply KB976749)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS09-072		
MS09-053	10/13/09	KB975254	Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution (975254)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-052	10/13/09	KB974112	Vulnerability in Windows Media Player Could Allow Remote Code Execution (974112) (Replaces MS08-076)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-051	10/14/09	KB954155 KB975025	Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution (975682) (Two updates required)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-050	10/14/09		Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)	No Longer Evaluated		Not Applicable		
MS09-049	09/09/09		Vulnerability in Wireless LAN AutoConfig Service Could Allow Remote Code Execution (970710)	No Longer Evaluated		Not Applicable		
MS09-048	09/10/09	KB967723	Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS11-058		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS09-047	09/08/09	KB968816	Vulnerabilities in Windows Media Format Could Allow Remote Code Execution (973812) (968816) (Replaces MS08-076)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS10-033		
MS09-046	09/08/09	KB956844	Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (956844)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-045	09/09/09		Vulnerability in Jscript Scripting Engine Could Allow Remote Code Execution (971961)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS11-031		
MS09-044	08/13/09	KB958469	Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (970927) (RDP version 5.2)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-043	08/12/09		Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution (957638)	No Longer Evaluated		Not Applicable		
MS09-042	08/12/09	KB960859	Vulnerability in Telnet Could Allow Remote Code Execution (960859)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-041	08/11/09	KB971657	Vulnerability in Workstation Service Could Allow Elevation of Privilege (971657)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-040	08/11/09	KB971032	Vulnerability in Message Queuing Could Allow Elevation of Privilege (971032)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-039	08/12/09	KB969883	Vulnerabilities in WINS Could Allow Remote Code Execution (969883) (Replaces MS09-008)	No Longer Evaluated		Not Applicable		
MS09-038	08/11/09	KB971557	Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution (971557)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS10-013		
MS09-037	08/11/09	KB973869 KB973507 KB973815 KB973540	Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908). KB973540 replaces MS07-047. CallPilot 3.0/4.0 also need KB973354	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-036	08/13/09		Vulnerability in ASP.NET in Microsoft Windows Could Allow Denial of Service (970957)	No Longer Evaluated		Not Applicable		
MS09-035	07/28/09		Vulnerabilities in Visual Studio Active Template Library Could Allow Remote Code Execution (969706)	No Longer Evaluated		Not Applicable		
MS09-034	07/28/09	KB972260	Cumulative Security Update for Internet Explorer (972260) (Replaces MS09-019)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS09-054		
MS09-033	07/15/09		Vulnerability in Virtual PC and Virtual Server Could Allow Elevation of Privilege (969856)	No Longer Evaluated		Not Applicable		
MS09-032	07/15/09	KB973346	Cumulative Security Update of ActiveX Kill Bits (973346) (Replaces MS08-032)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS09-055		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS09-031	07/14/09		Vulnerability in Microsoft ISA Server 2006 Could Cause Elevation of Privilege (970953)	No Longer Evaluated		Not Applicable		
MS09-030	07/15/09		Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (969516)	No Longer Evaluated		Not Applicable		
MS09-029	07/15/09	KB961371	Vulnerabilities in the Embedded OpenType Font Engine Could Allow Remote Code Execution (961371)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS10-001		
MS09-028	07/14/09	KB971633	Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution (971633) (Replaces MS09-011)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS10-033		
MS09-027	06/09/09		Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (969514)	No Longer Evaluated		Not Applicable		
MS09-026	06/09/09	KB970238	Vulnerability in RPC Could Allow Elevation of Privilege (970238) (Replaces MS07-058)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS10-066		
MS09-025	06/09/09	KB968537	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537) (Replaces MS09-006)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS09-065		
MS09-024	06/09/09		Vulnerability in Microsoft Works Converters Could Allow Remote Code Execution (957632)	No Longer Evaluated		Not Applicable		
MS09-023	06/09/09		Vulnerability in Windows Search Could Allow Information Disclosure (963093)	No Longer Evaluated		Not Applicable		
MS09-022	06/09/09	KB961501	Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
						Superseded by MS12-054		
MS09-021	06/09/09		Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)	No Longer Evaluated		Not Applicable		
MS09-020	06/09/09	KB970483	Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-019	06/10/09	KB969897	Cumulative Security Update for Internet Explorer (969897) (Replaces MS09-014)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS09-034		
MS09-018	06/09/09		Vulnerabilities in Active Directory Could Allow Remote Code Execution (971055)	No Longer Evaluated		Not Applicable		
MS09-017	5/12/09		Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	No Longer Evaluated		Not Applicable		
MS09-016	04/14/09		Vulnerabilities in Microsoft ISA Server and Forefront Threat Management Gateway (Medium Business Edition) Could Cause Denial of Service (961759)	No Longer Evaluated		Not Applicable		
MS09-015	04/15/09	KB959426	Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426) (Replaces MS07-035)	No Longer Evaluated		SEC012S	SEC012S	SEC012S

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS09-014	04/15/09	KB963027	Cumulative Security Update for Internet Explorer (963027) (Replaces MS08-073 and MS08-078)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS09-019		
MS09-013	04/14/09	KB960803	Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-012	04/15/09	KB956572 KB952004	Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)	No Longer Evaluated		SEC012S Note 5	SEC012S Note 5	SEC012S Note 5
MS09-011	04/14/09	KB961373	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (961373) (Replaces MS08-033)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS09-028		
MS09-010	04/16/09	KB923561	Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (960477)	No Longer Evaluated		SEC012S Note 6	SEC012S Note 6	SEC012S Note 6
MS09-009	04/14/09		Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution (968557)	No Longer Evaluated		Not Applicable		
MS09-008	03/11/09		Vulnerabilities in DNS and WINS Server Could Allow Spoofing (962238)	No Longer Evaluated		Not Applicable		
MS09-007	03/10/09	KB960225	Vulnerability in Schannel Could Allow Spoofing (960225) (Replaces MS07-031)	No Longer Evaluated		SEC012S	SEC012S	SEC012S
MS09-006	03/10/09	KB958690	Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690) (Replaces MS08-061)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS09-025		
MS09-005	02/10/09		Vulnerabilities in Microsoft Office Visio Could Allow Remote Code Execution (957634)	No Longer Evaluated		Not Applicable		
MS09-004	02/10/09		Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420)	No Longer Evaluated		Not Applicable		
MS09-003	02/10/09		Vulnerabilities in Microsoft Exchange Could Allow Remote Code Execution (959239)	No Longer Evaluated		Not Applicable		
MS09-002	02/10/09		Cumulative Security Update for Internet Explorer (961260)	No Longer Evaluated		Not Applicable		
MS09-001	01/13/09	KB958687	Vulnerabilities in SMB Could Allow Remote Code Execution (958687) (Replaces MS08-063)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS10-012		
MS08-078	12/18/08	KB960714	Security Update for Internet Explorer (960714)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS09-014		
MS08-077	12/09/08		Vulnerability in Microsoft Office SharePoint Server Could Cause Elevation of Privilege (957175)	No Longer Evaluated		Not Applicable		
MS08-076	12/10/08	KB954600 KB952069	Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (959807)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS09-052		
MS08-075	12/10/08		Vulnerabilities in Windows Search Could Allow Remote Code Execution (959349)	No Longer Evaluated		Not Applicable		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS08-074	12/09/08		Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (959070)	No Longer Evaluated		Not Applicable		
MS08-073	12/09/08	KB958215	Cumulative Security Update for Internet Explorer (958215) (Replaces MS08-058)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS09-014		
MS08-072	12/09/08		Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (957173)	No Longer Evaluated		Not Applicable		
MS08-071	12/10/08	KB956802	Vulnerabilities in GDI Could Allow Remote Code Execution (956802) (Replaces MS08-021)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
MS08-070	12/09/08		Vulnerabilities in Visual Basic 6.0 Runtime Extended Files (ActiveX Controls) Could Allow Remote Code Execution (932349)	No Longer Evaluated		Not Applicable		
MS08-069	12/10/08		Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (955218) (Replaces MS07-042)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS10-051		
MS08-068	11/12/08	KB957097	Vulnerability in SMB Could Allow Remote Code Execution (957097)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS10-006		
MS08-067	10/23/08	KB958644	Vulnerability in Server Service Could Allow Remote Code Execution (958644) (Replaces MS06-040)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS12-054		
MS08-066	10/14/08	KB956803	Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege (956803)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS11-030		
MS08-065	10/15/08		Vulnerability in Message Queuing Could Allow Remote Code Execution (951071)	No Longer Evaluated		Not Applicable		
MS08-064	10/15/08	KB956841	Vulnerability in Virtual Address Descriptor Manipulation Could Allow Elevation of Privilege (956841) (Replaces MS07-022)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS09-0058		
MS08-063	10/15/08		Vulnerability in SMB Could Allow Remote Code Execution (957095)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS09-001		
MS08-062	10/16/08	KB953155	Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution (953155)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
MS08-061	10/14/08	KB954211	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (954211) (Replaces MS08-025)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS09-006		
MS08-060	10/15/08		Vulnerability in Active Directory Could Allow Remote Code Execution (957280)	No Longer Evaluated		Not Applicable		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS08-059	10/15/08		Vulnerability in Host Integration Server RPC Service Could Allow Remote Code Execution (956695)	No Longer Evaluated		Not Applicable		
MS08-058	10/15/08	KB956390	Cumulative Security Update for Internet Explorer (956390) (Replaces MS08-045)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS08-073		
MS08-057	10/15/08		Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (956416)	No Longer Evaluated		Not Applicable		
MS08-056	10/14/08		Vulnerability in Microsoft Office Could Allow Information Disclosure (957699)	No Longer Evaluated		Not Applicable		
MS08-055	09/10/08		Vulnerability in Microsoft Office Could Allow Remote Code Execution (955047)	No Longer Evaluated		Not Applicable		
MS08-054	09/10/08		Vulnerability in Windows Media Player Could Allow Remote Code Execution (954154)	No Longer Evaluated		Not Applicable		
MS08-053	09/10/08		Vulnerability in Windows Media Encoder 9 Could Allow Remote Code Execution (954156)	No Longer Evaluated		Not Applicable		
MS08-052	09/09/08	KB938464	Vulnerabilities in GDI+ Could Allow Remote Code Execution (938464)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS08-062		
MS08-051	08/13/08		Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (949785)	No Longer Evaluated		Not Applicable		
MS08-050	08/12/08		Vulnerability in Windows Messenger Could Allow Information Disclosure (955702)	No Longer Evaluated		Not Applicable		
MS08-049	08/12/08	KB950974	Vulnerabilities in Event System Could Allow Remote Code Execution (950974)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
MS08-048	08/13/08	KB951066	Security Update for Outlook Express and Windows Mail (951066)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
MS08-047	08/13/08		Vulnerability in Ipsec Policy Processing Could Allow Information Disclosure (953733)	No Longer Evaluated		Not Applicable		
MS08-046	08/12/08	KB952954	Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution (952954)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
MS08-045	08/12/08	KB953838	Cumulative Security Update for Internet Explorer (953838) (Replaces MS08-031)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS08-058		
MS08-044	08/13/08		Vulnerabilities in Microsoft Office Filters Could Allow Remote Code Execution (924090)	No Longer Evaluated		Not Applicable		
MS08-043	08/13/08		Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (954066)	No Longer Evaluated		Not Applicable		
MS08-042	08/12/08		Vulnerability in Microsoft Word Could Allow Remote Code Execution (955048)	No Longer Evaluated		Not Applicable		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS08-041	08/12/08		Vulnerability in the ActiveX Control for the Snapshot Viewer for Microsoft Access Could Allow Remote Code Execution (955617)	No Longer Evaluated		Not Applicable		
MS08-040	07/09/09		Vulnerabilities in Microsoft SQL Server Could Allow Elevation of Privilege (941203)	No Longer Evaluated		Not Applicable		
MS08-039	07/09/08		Vulnerabilities in Outlook Web Access for Exchange Server Could Allow Elevation of Privilege (953747)	No Longer Evaluated		Not Applicable		
MS08-038	07/08/08		Vulnerability in Windows Explorer Could Allow Remote Code Execution (950582)	No Longer Evaluated		Not Applicable		
MS08-037	07/08/08	KB951748	Vulnerabilities in DNS Could Allow Spoofing (953230) (951748)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS11-030		
MS08-036	06/10/08	KB950762	Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service (950762)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
MS08-035	06/11/08		Vulnerability in Active Directory Could Allow Denial of Service (953235)	No Longer Evaluated		Not Applicable		
MS08-034	06/11/08		Vulnerability in WINS Could Allow Elevation of Privilege (948745)	No Longer Evaluated		Not Applicable		
MS08-033	06/10/08	KB951698	Vulnerabilities in DirectX Could Allow Remote Code Execution (951698) (Replaces MS07-064)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS09-011		
MS08-032	06/10/08	KB950760	Cumulative Security Update of ActiveX Kill Bits (950760) (Replaces MS08-023)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS09-032		
MS08-031	06/11/08		Cumulative Security Update for Internet Explorer (950759) (Replaces MS08-024)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS08-045		
MS08-030	06/10/08		Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (951376)	No Longer Evaluated		Not Applicable		
MS08-029	05/13/08		Vulnerabilities in Microsoft Malware Protection Engine Could Allow Denial of Service (952044)	No Longer Evaluated		Not Applicable		
MS08-028	05/13/08	KB950749	Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution (950749)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Does not apply if PEP CPSECPEPSP2S (Windows Server 2003/SP2) has been installed		
MS08-027	05/13/08		Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (951208)	No Longer Evaluated		Not Applicable		
MS08-026	05/14/08		Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (951207)	No Longer Evaluated		Not Applicable		
MS08-025	04/09/08	KB941693	Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS08-061		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS08-024	04/08/08		Cumulative Security Update for Internet Explorer (947864) (Replaces MS08-010)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS08-031		
MS08-023	04/23/08	KB948881	Security Update of ActiveX Kill Bits (948881)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS08-032		
MS08-022	08/12/08	KB944338	Vulnerability in VBScript and Jscript Scripting Engines Could Allow Remote Code Execution (944338) (Replaces MS06-023)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
MS08-021	04/09/08	KB948590	Vulnerabilities in GDI Could Allow Remote Code Execution (948590) (Replaces MS07-046)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS08-071		
MS08-020	04/09/08	KB945553	Vulnerability in DNS Client Could Allow Spoofing (945553)	No Longer Evaluated		SEC011S	SEC011S	SEC011S
						Superseded by MS11-030		
MS08-019	04/08/08		Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (949032)	No Longer Evaluated		Not Applicable		
MS08-018	04/08/08		Vulnerability in Microsoft Project Could Allow Remote Code Execution (950183)	No Longer Evaluated		Not Applicable		
MS08-017	03/11/08		Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution (933103)	No Longer Evaluated		Not Applicable		
MS08-016	03/11/08		Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (949030)	No Longer Evaluated		Not Applicable		
MS08-015	03/11/08		Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (949031)	No Longer Evaluated		Not Applicable		
MS08-014	03/11/08		Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (949029)	No Longer Evaluated		Not Applicable		
MS08-013	02/13/08		Vulnerability in Microsoft Office Could Allow Remote Code Execution (947108)	No Longer Evaluated		Not Applicable		
MS08-012	02/13/08		Vulnerabilities in Microsoft Office Publisher Could Allow Remote Code Execution (947085)	No Longer Evaluated		Not Applicable		
MS08-011	02/12/08		Vulnerabilities in Microsoft Works File Converter Could Allow Remote Code Execution (947081)	No Longer Evaluated		Not Applicable		
MS08-010	02/13/08		Cumulative Security Update for Internet Explorer (944533) (Replaces MS07-069)	No Longer Evaluated		SEC010S	SEC010S	SEC010S
						Superseded by MS08-024		
MS08-009	02/12/08		Vulnerability in Microsoft Word Could Allow Remote Code Execution (947077)	No Longer Evaluated		Not Applicable		
MS08-008	02/13/08	KB943055	Vulnerability in OLE Automation Could Allow Remote Code Execution (943055) (Replaces MS07-043)	No Longer Evaluated		SEC010S, Note 4	SEC010S, Note 4	SEC010S, Note 4
						Superseded by MS11-038		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS08-007	02/13/08	KB946026	Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026)	No Longer Evaluated		SEC010S	SEC010S	SEC010S
MS08-006	02/12/08	KB942830	Vulnerability in Internet Information Services Could Allow Remote Code Execution (942830) (Replaces MS06-034)	No Longer Evaluated		SEC010S	SEC010S	SEC010S
						Superseded by MS10-065		
MS08-005	02/13/08	KB942831	Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831)	No Longer Evaluated		SEC010S	SEC010S	SEC010S
MS08-004	02/12/08		Vulnerability in Windows TCP/IP Could Allow Denial of Service (946456)	No Longer Evaluated		Not Applicable		
MS08-003	02/13/08		Vulnerability in Active Directory Could Allow Denial of Service (946538)	No Longer Evaluated		Not Applicable		
MS08-002	01/08/08	KB943485	Vulnerability in LSASS Could Allow Local Elevation of Privilege (943485)	No Longer Evaluated		SEC010S	SEC010S	SEC010S
						Superseded by MS11-014		
MS08-001	01/08/08	KB941644	Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (941644) (Replaces MS06-032)	No Longer Evaluated		SEC010S	SEC010S	SEC010S
MS07-069	12/12/07	KB942615	Cumulative Security Update for Internet Explorer (942615)	No Longer Evaluated		Approved	Approved	Approved
						Superseded by MS08-010		
MS07-068	12/11/07	KB941569	Vulnerability in Windows Media File Format Could Allow Remote Code Execution (941569 and 944275)	No Longer Evaluated		SEC010S	SEC010S	SEC010S
MS07-067	12/11/07	KB944653	Vulnerability in Macrovision Driver Could Allow Local Elevation of Privilege (944653)	No Longer Evaluated		SEC010S	SEC010S	SEC010S
MS07-066	12/12/07		Vulnerability in Windows Kernel Could Allow Elevation of Privilege (943078)	No Longer Evaluated		Not Applicable		
MS07-065	12/11/07		Vulnerability in Message Queuing Could Allow Remote Code Execution (937894)	No Longer Evaluated		Not Applicable		
MS07-064	12/12/07	KB941568	Vulnerabilities in DirectX Could Allow Remote Code Execution (941568) (Replaces MS05-060)	No Longer Evaluated		SEC010S	SEC010S	SEC010S
						Superseded by MS08-033		
MS07-063	12/11/07		Vulnerability in SMBv2 Could Allow Remote Code Execution (942624)	No Longer Evaluated		Not Applicable		
MS07-062	11/13/07	KB941672	Vulnerability in DNS Could Allow Spoofing (941672)	No Longer Evaluated		Not Applicable		
MS07-061	11/13/07	KB943460	Vulnerability in Windows URI Handling Could Allow Remote Code Execution (943460) (Replaces MS06-045)	No Longer Evaluated		SEC009S	SEC009S	SEC009S
MS07-060	10/10/07		Vulnerability in Microsoft Word Could Allow Remote Code Execution (942695)	No Longer Evaluated		Not Applicable		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS07-059	10/09/07		Vulnerability in Windows SharePoint Services 3.0 and Office SharePoint Server 2007 Could Result in Elevation of Privilege Within the SharePoint Site (942017)	No Longer Evaluated		Not Applicable		
MS07-058	10/10/07	KB933729	Vulnerability in RPC Could Allow Denial of Service (933729)	No Longer Evaluated		SEC009S	SEC009S	SEC009S
						Superseded by MS09-026		
MS07-057	10/10/07	KB939653	Cumulative Security Update for Internet Explorer (939653)	No Longer Evaluated		SEC009S	SEC009S	SEC009S
						Superseded by MS07-069		
MS07-056	10/10/07	KB941202	Security Update for Outlook Express and Windows Mail (941202)	No Longer Evaluated		SEC009S	SEC009S	SEC009S
MS07-055	10/09/07		Vulnerability in Kodak Image Viewer Could Allow Remote Code Execution (923810)	No Longer Evaluated		Not Applicable		
MS07-054	09/11/07		Vulnerability in MSN Messenger and Windows Live Messenger Could Allow Remote Code Execution (942099)	No Longer Evaluated		Not Applicable		
MS07-053	09/11/07		Vulnerability in Windows Services for UNIX Could Allow Elevation of Privilege (939778)	No Longer Evaluated		Not Applicable		
MS07-052	09/11/07		Vulnerability in Crystal Reports for Visual Studio Could Allow Remote Code Execution (941522)	No Longer Evaluated		Not Applicable		
MS07-051	09/11/07		Vulnerability in Microsoft Agent Could Allow Remote Code Execution (938827)	No Longer Evaluated		Not Applicable		
MS07-050	08/15/07	KB938127	Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)	No Longer Evaluated		SEC008S	SEC008S	SEC008S
MS07-049	08/14/07		Vulnerability in Virtual PC and Virtual Server Could Allow Elevation of Privilege (937986)	No Longer Evaluated		Not Applicable		
MS07-048	08/14/07		Vulnerabilities in Windows Gadgets Could Allow Remote Code Execution (938123)	No Longer Evaluated		Not Applicable		
MS07-047	08/14/07		Vulnerabilities in Windows Media Player Could Allow Remote Code Execution (936782)	No Longer Evaluated		SEC008S	SEC008S	SEC008S
						Superseded by MS09-037		
MS07-046	08/14/07	KB938829	Vulnerability in GDI Could Allow Remote Code Execution (938829)	No Longer Evaluated		SEC008S	SEC008S	SEC008S
						Superseded by MS08-021		
MS07-045	08/14/07	KB937143	Cumulative Security Update for Internet Explorer (937143)	No Longer Evaluated		SEC008S	SEC008S	SEC008S
						Superseded by MS07-057		
MS07-044	08/14/07		Vulnerability in Microsoft Excel Could Allow Remote Code Execution (940965)	No Longer Evaluated		Not Applicable		
MS07-043	08/14/07	KB921503	Vulnerability in OLE Automation Could Allow Remote Code Execution (921503)	No Longer Evaluated		SEC008S	SEC008S	SEC008S
						Superseded by MS08-008		

<table>
<tr><th colspan="4">Microsoft Security Update Details</th><th colspan="5">CallPilot Release</th></tr>
<tr><th>Bulletin #</th><th>Date</th><th>Hotfix</th><th>Description</th><th>2.02</th><th>2.5</th><th>3.0</th><th>4.0</th><th>5.0/5.1</th></tr>
<tr><td rowspan="2">MS07-042</td><td rowspan="2">08/15/07</td><td rowspan="2">KB936021</td><td rowspan="2">Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227)</td><td colspan="2" rowspan="2">No Longer Evaluated</td><td>SEC008S</td><td>SEC008S</td><td>SEC008S</td></tr>
<tr><td colspan="3">Superseded by MS08-069</td></tr>
<tr><td>MS07-041</td><td>07/12/07</td><td></td><td>Vulnerability in Microsoft Internet Information Services Could Allow Remote Code Execution (939373)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td>MS07-040</td><td>07/12/07</td><td>KB933854</td><td>Vulnerabilities in .NET Framework Could Allow Remote Code Execution (933854)</td><td colspan="2">No Longer Evaluated</td><td>SEC008S</td><td>SEC008S</td><td>SEC008S</td></tr>
<tr><td>MS07-039</td><td>07/12/07</td><td>KB926122</td><td>Vulnerability in Windows Active Directory Could Allow Remote Code Execution (926122)</td><td colspan="2">No Longer Evaluated</td><td>SEC008S</td><td>SEC008S</td><td>SEC008S</td></tr>
<tr><td>MS07-038</td><td>07/12/07</td><td></td><td>Vulnerability in Windows Vista Firewall Could Allow Information Disclosure (935807)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td>MS07-037</td><td>07/10/07</td><td></td><td>Vulnerability in Microsoft Office Publisher 2007 Could Allow Remote Code Execution (936548)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td>MS07-036</td><td>07/12/07</td><td></td><td>Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (936542)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td rowspan="2">MS07-035</td><td rowspan="2">06/12/07</td><td rowspan="2"></td><td rowspan="2">Vulnerability in Win 32 API Could Allow Remote Code Execution (935839)</td><td colspan="2" rowspan="2">No Longer Evaluated</td><td>SEC007S</td><td>SEC007S</td><td>SEC007S</td></tr>
<tr><td colspan="3">Superseded by MS09-015</td></tr>
<tr><td>MS07-034</td><td>06/13/07</td><td>KB929123</td><td>Cumulative Security Update for Outlook Express and Windows Mail (929123)</td><td colspan="2">No Longer Evaluated</td><td>SEC007S</td><td>SEC007S</td><td>SEC007S</td></tr>
<tr><td rowspan="2">MS07-033</td><td rowspan="2">06/13/07</td><td rowspan="2">KB933566</td><td rowspan="2">Cumulative Security Update for Internet Explorer (933566)</td><td colspan="2" rowspan="2">No Longer Evaluated</td><td>SEC007S</td><td>SEC007S</td><td>SEC007S</td></tr>
<tr><td colspan="3">Superseded by MS07-045</td></tr>
<tr><td>MS07-032</td><td>06/12/07</td><td></td><td>Vulnerability in Windows Vista Could Allow Information Disclosure (931213)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td rowspan="2">MS07-031</td><td rowspan="2">06/12/07</td><td rowspan="2">KB935840</td><td rowspan="2">Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840)</td><td colspan="2" rowspan="2">No Longer Evaluated</td><td>SEC007S</td><td>SEC007S</td><td>SEC007S</td></tr>
<tr><td colspan="3">Superseded by MS09-007</td></tr>
<tr><td>MS07-030</td><td>06/12/07</td><td></td><td>Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (927051)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td rowspan="2">MS07-029</td><td rowspan="2">05/08/07</td><td rowspan="2">KB941672</td><td rowspan="2">Vulnerability in Windows DNS RPC Interface Could Allow Remote Code Execution (935966)</td><td colspan="2" rowspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td colspan="3">Superseded by MS07-062</td></tr>
<tr><td>MS07-028</td><td>05/08/07</td><td></td><td>Vulnerability in CAPICOM Could Allow Remote Code Execution (931906)</td><td colspan="2">No Longer Evaluated</td><td>SEC009S</td><td>SEC009S</td><td>SEC009S</td></tr>
<tr><td rowspan="2">MS07-027</td><td rowspan="2">05/08/07</td><td rowspan="2">KB931768</td><td rowspan="2">Cumulative Security Update for Internet Explorer (931768) (Replaces MS07-016)</td><td colspan="2" rowspan="2">No Longer Evaluated</td><td>Approved</td><td>Approved</td><td>Approved</td></tr>
<tr><td colspan="3">Superseded by MS07-033</td></tr>
<tr><td>MS07-026</td><td>05/08/07</td><td></td><td>Vulnerabilities in Microsoft Exchange Could Allow Remote Code Execution (931832)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
<tr><td>MS07-025</td><td>05/08/07</td><td></td><td>Vulnerability in Microsoft Office Could Allow Remote Code Execution (934873)</td><td colspan="2">No Longer Evaluated</td><td colspan="3">Not Applicable</td></tr>
</table>

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS07-024	05/08/07		Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (934232)	No Longer Evaluated		Not Applicable		
MS07-023	05/08/07		Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (934233)	No Longer Evaluated		Not Applicable		
MS07-022	04/10/07	KB931784	Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784)	No Longer Evaluated		SEC006S	SEC006S	SEC006S
						Superseded by MS08-064		
MS07-021	04/10/07	KB930178	Vulnerabilities in CSRSS Could Allow Remote Code Execution (930178)	No Longer Evaluated		SEC006S	SEC006S	SEC006S
						Superseded by MS10-069		
MS07-020	04/10/07	KB932168	Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168)	No Longer Evaluated		SEC006S	SEC006S	SEC006S
MS07-019	04/10/07		Vulnerability in Universal Plug and Play Could Allow Remote Code Execution (931261)	No Longer Evaluated		Not Applicable		
MS07-018	04/10/07		Vulnerabilities in Microsoft Content Management Server Could Allow Remote Code Execution (925939)	No Longer Evaluated		Not Applicable		
MS07-017	04/03/07	KB925902	Vulnerabilities in GDI Could Allow Remote Code Execution (925902)	No Longer Evaluated		SEC006S	SEC006S	SEC006S
MS07-016	02/13/07	KB928090	Cumulative Security Update for Internet Explorer (928090) (Replaces MS06-072)	No Longer Evaluated		SEC006S	SEC006S	SEC006S
						Superseded by MS07-027		
MS07-015	02/13/07		Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (932554)	No Longer Evaluated		Not Applicable		
MS07-014	02/13/07		Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (929434)	No Longer Evaluated		Not Applicable		
MS07-013	02/13/07	KB918118	Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution (918118)	No Longer Evaluated		SEC006S	SEC006S	SEC006S
MS07-012	02/13/07	KB924667	Vulnerability in Microsoft MFC Could Allow Remote Code Execution (924667)	No Longer Evaluated		SEC006S	SEC006S	SEC006S
						See note 3 for additional step required after reboot Superseded by MS10-074		
MS07-011	02/13/07	KB926436	Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution (926436)	No Longer Evaluated		SEC006S	SEC006S	SEC006S
MS07-010	02/13/07		Vulnerability in Microsoft Malware Protection Engine Could Allow Remote Code Execution (932135)	No Longer Evaluated		Not Applicable		
MS07-009	02/13/07		Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (927779)	No Longer Evaluated		Approved, Not Applicable if SECSP1S PEP has been applied	Not Applicable	

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS07-008	02/13/07	KB928843	Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843)	No Longer Evaluated		SEC006S	SEC006S	SEC006S
MS07-007	02/13/07		Vulnerability in Windows Image Acquisition Service Could Allow Elevation of Privilege (927802)	No Longer Evaluated		Not Applicable		
MS07-006	02/15/07	KB928255	Vulnerability in Windows Shell Could Allow Elevation of Privilege (928255)	No Longer Evaluated		SEC006S	SEC006S	SEC006S
MS07-005	02/13/07		Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution (923723)	No Longer Evaluated		Not Applicable		
MS07-004	01/09/07		Vulnerability in Vector Markup Language Could Allow Remote Code Execution (929969)	No Longer Evaluated		SEC006S	SEC006S	SEC006S
MS07-003	01/09/07		Vulnerabilities in Microsoft Outlook Could Allow Remote Code Execution (925938)	No Longer Evaluated		Not Applicable		
MS07-002	01/09/07		Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (927198)	No Longer Evaluated		Not Applicable		
MS07-001	01/09/07		Vulnerability in Microsoft Office 2003 Brazilian Portuguese Grammar Checker That Could Allow Remote Code Execution (921585)	No Longer Evaluated		Not Applicable		
MS06-078	12/12/06	KB923689 KB925398	Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689) (Requires two updates: WMF 7.1-9.5 and WMP 6.4 (925398)	No Longer Evaluated		SEC006S	SEC006S	√
MS06-077	12/12/06		Vulnerability in Remote Installation Service Could Allow Remote Code Execution (926121)	Not Applicable				
MS06-076	12/12/06	KB923694	Cumulative Security Update for Outlook Express (923694)	No Longer Evaluated		SEC006S	SEC006S	√
MS06-075	12/12/06	KB926255	Vulnerability in Windows Could Allow Elevation of Privilege (926255)	Not Applicable		Approved, Not Applicable if SECSP1S PEP has been applied	SEC006S	√
MS06-074	12/12/06	KB926247	Vulnerability in SNMP Could Allow Remote Code Execution (926247)	Not Applicable		SEC006S	SEC006S	√
MS06-073	12/12/06		Vulnerability in Visual Studio 2005 Could Allow Remote Code Execution (925674)	Not Applicable				
MS06-072	12/12/06	KB925454	Cumulative Security Update for Internet Explorer (925454) (Replaces MS06-067)	Not Applicable		SEC006S	SEC006S	√
						Superseded by MS07-016		
MS06-071	11/14/06		Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (928088). (May require KB927978 depending on version of MSXML installed which is also "Approved" for use.)	Not Applicable				

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS06-070	11/14/06		Vulnerability in Workstation Service Could Allow Remote Code Execution (924270)	Not Applicable				
MS06-069	11/14/06		Vulnerabilities in Macromedia Flash Player from Adobe Could Allow Remote Code Execution (923789)	Not Applicable				
MS06-068	11/14/06	KB920213	Vulnerability in Microsoft Agent Could Allow Remote Code Execution (920213)	Not Applicable		SEC006S	SEC006S	√
MS06-067	11/14/06	KB922760	Cumulative Security Update for Internet Explorer (922760) (Replaces MS06-042)	Not Applicable		Approved	Approved	√
						Superseded by MS06-072		
MS06-066	11/14/06	KB923980	Vulnerabilities in Client Service for NetWare Could Allow Remote Code Execution (923980)	Not Applicable		SEC006S	SEC006S	√
MS06-065	10/10/06	KB924496	Vulnerability in Windows Object Packager Could Allow Remote Execution (924496)	Not Applicable		SEC005S	SEC005S	√
MS06-064	10/10/06	KB922819	Vulnerabilities in TCP/IP Ipv6 Could Allow Denial of Service (922819)	Not Applicable		SEC005S	SEC005S	√
MS06-063	10/11/06		Vulnerability in Server Service Could Allow Denial of Service and Remote Code Execution (923414)	Approved	Approved	SEC005S	SEC005S	√
MS06-062	10/11/06		Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (922581)	Not Applicable				
MS06-061	10/11/06	KB924191	Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (924191) (May require KB925672 depending on version of MSXML installed. KB925672 is also "Approved" for use.)	Not Applicable		SEC005S	SEC005S	√
MS06-060	10/11/06		Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (924554)	Not Applicable				
MS06-059	10/10/06		Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (924164)	Not Applicable				
MS06-058	10/10/06		Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (924163)	Not Applicable				
MS06-057	10/10/06	KB923191	Vulnerability in Windows Explorer Could Allow Remote Execution (923191)	Not Applicable		SEC005S	SEC005S	√
MS06-056	10/11/06		Vulnerability in ASP.NET 2.0 Could Allow Information Disclosure (922770)	Not Applicable				
MS06-055	09/26/06	KB925486	Vulnerability in Vector Markup Language Could Allow Remote Code Execution (925486)	Not Applicable		SEC005S	SEC005S	√
MS06-054	09/12/06		Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (910729)	Not Applicable				
MS06-053	09/12/06	KB920685	Vulnerability in Indexing Service Could Allow Cross-Site Scripting (920685)	Not Applicable		SEC005S	SEC005S	√
MS06-052	09/12/06		Vulnerability in Pragmatic General Multicast (PGM) Could Allow Remote Code Execution (919007)	Not Applicable				

Microsoft Security Update Details				CallPilot Release				
Bulletin #	**Date**	**Hotfix**	**Description**	**2.02**	**2.5**	**3.0**	**4.0**	**5.0/5.1**
MS06-042 (revised)	09/12/06	KB918899	Cumulative Security Update for Internet Explorer (918899)	Not Applicable		SEC005S	SEC005S	√
MS06-040 (revised)	09/12/06	KB921883	Vulnerability in Server Service Could Allow Remote Code Execution (921883)	Not Applicable		SEC005S	SEC005S	√
MS06-051	08/08/06	KB917422	Vulnerability in Windows Kernel Could Result in Remote Code Execution (917422)	Approved	Approved	SEC005S	SEC005S	√
MS06-050	08/08/06	KB920670	Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution (920670)	Approved	Approved	SEC005S	SEC005S	√
MS06-049	08/08/06		Vulnerability in Windows Kernel Could Result in Elevation of Privilege (920958)	Approved	Approved	Not Applicable		
MS06-048	08/08/06		Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (922968)	Not Applicable				
MS06-047	08/08/06		Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (921645)	Not Applicable				
MS06-046	08/08/06	KB922616	Vulnerability in HTML Help Could Allow Remote Code Execution (922616)	Not Applicable		SEC005S	SEC005S	√
MS06-045	08/08/06	KB921398	Vulnerability in Windows Explorer Could Allow Remote Code Execution (921398)	Approved	Approved	SEC005S	SEC005S	√
						Superseded by MS07-061		
MS06-044	08/08/06		Vulnerability in Microsoft Management Console Could Allow Remote Code Execution (917008)	Not Applicable				
MS06-043	08/08/06		Vulnerability in Microsoft Windows Could Allow Remote Code Execution (920214)	Not Applicable		SEC005S	SEC005S	√
MS06-042	08/08/06	KB918899	Cumulative Security Update for Internet Explorer (918899) (Replaces MS06-021)	Not Applicable		Approved	Approved	Not Applicable
						Revised 09/12/06		
MS06-041	08/08/06	KB920683	Vulnerabilities in DNS Resolution Could Allow Remote Code Execution (920683)	Approved	Approved	SEC005S	SEC005S	√
MS06-040	08/08/06	KB921883	Vulnerability in Server Service Could Allow Remote Code Execution (921883)	Approved	Approved	Approved	Approved	Not Applicable
						Revised 09/12/06, Superseded by MS08-067		
MS06-039	07/12/06		Vulnerabilities in Microsoft Office Filters Could Allow Remote Code Execution (915384)	Not Applicable				
MS06-038	07/12/06		Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (917284)	Not Applicable				
MS06-037	07/12/06		Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (917285)	Not Applicable				
MS06-036	07/11/06	KB914388	Vulnerability in DHCP Client Service Could Allow Remote Code Execution (914388)	Not Applicable		SEC005S	SEC005S	√
MS06-035	07/12/06		Vulnerability in Server Service Could Allow Remote Code Execution (917159)	Approved	Approved	SEC005S	SEC005S	√

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS06-034	07/12/06	KB917537	Vulnerability in Microsoft Internet Information Services using Active Server Pages Could Allow Remote Code Execution (917537)	Not Applicable		SEC005S	SEC005S	√
						Superseded by MS08-006		
MS06-033	07/11/06		Vulnerability in ASP.NET Could Allow Information Disclosure (917283)	Not Applicable				
MS06-032	06/13/06	KB917953	Vulnerability in TCP/IP Could Allow Remote Code Execution (917953)	Not Applicable		SEC005S	SEC005S	√
						Superseded by MS08-001		
MS06-031	06/13/06		Vulnerability in RPC Mutual Authentication Could Allow Spoofing (917736)	Not Applicable				
MS06-030	06/14/06	KB914389	Vulnerability in Server Message Block Could Allow Elevation of Privilege (914389)	Not Applicable		SEC005S	SEC005S	√
MS06-029	06/13/06		Vulnerability in Microsoft Exchange Server Running Outlook Web Access Could Allow Script Injection (912442)	Not Applicable				
MS06-028	06/14/06		Vulnerability in Microsoft PowerPoint Could Allow Remote Code Execution (916768)	Not Applicable				
MS06-027	06/14/06		Vulnerability in Microsoft Word Could Allow Remote Code Execution (917336)	Not Applicable				
MS06-026	06/13/06		Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution (918547)	Not Applicable				
MS06-025	06/13/06		Vulnerability in Routing and Remote Access Could Allow Remote Code Execution (911280)	SEC004S	Approved	SEC005S	SEC005S	√
MS06-024	06/13/06		Vulnerability in Windows Media Player Could Allow Remote Code Execution (917734)	Not Applicable		SEC005S	SEC005S	√
MS06-023	06/13/06		Vulnerability in Microsoft Jscript Could Allow Remote Code Execution (917344)	SEC004S	Approved	SEC005S	SEC005S	√
						Superseded by MS08-022		
MS06-022	06/13/06	KB918439	Vulnerability in ART Image Rendering Could Allow Remote Code Execution (918439)	Not Applicable		SEC005S	SEC005S	√
MS06-021	06/14/06	KB916281	Cumulative Security Update for Internet Explorer (916281) (Replaces MS06-013)	Not Applicable		Approved	Approved	Not Applicable
						Revised 08/08/06		
MS06-011 (revised)	06/13/06		Permissive Windows Services DACLS Could Allow Elevation of Privilege (914798)	Not Applicable		Approved, Not Applicable if SECSP1S PEP has been applied	Not Applicable	
MS06-020	05/09/06		Vulnerabilities in Macromedia Flash Player from Adobe Could Allow Remote Code Execution (913433)	Not Applicable				
MS06-019	05/09/06		Vulnerability in Microsoft Exchange Could Allow Remote Code Execution (916803)	Not Applicable				

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS06-018	05/09/06		Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow Denial of Service (913580)	SEC004S	Approved	Approved, Not Applicable if SECSP1S PEP has been applied	Not Applicable	
MS06-017	04/11/06		Vulnerability in Microsoft FrontPage Server Extensions Could Allow Cross-Site Scripting (917627)	Not Applicable				
MS06-016	04/11/06		Cumulative Security Update for Outlook Express (911567)	Not Applicable		SEC004S	SEC004S	√
MS06-015	04/11/06		Vulnerability in Windows Explorer Could Allow Remote Code Execution (908531) (Replaces MS05-016 and MS05-008)	SEC004S	Approved	SEC004S	SEC004S	√
MS06-014	04/11/06		Vulnerability in Microsoft Data Access Components (MDAC) Function Could Allow Code Execution (911562)	SEC004S Requires MDAC 2.8/SP1 be installed first	Approved	SEC004S	SEC004S	√
MS06-013	04/11/06	KB912812	Cumulative Security Update for Internet Explorer (912812) (Replaces MS05-054)	Not Applicable		SEC004S	SEC004S	√
MS06-012	03/14/06		Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (905413)	Not Applicable				
MS06-011	03/14/06		Permissive Windows Services DACLs Could Allow Elevation of Privilege (914798)	Not Applicable		Approved, Not Applicable if SECSP1S PEP has been applied	Not Applicable	
MS06-010	02/14/06		Vulnerability in PowerPoint 2000 Could Allow Information Disclosure (889167)	Not Applicable				
MS06-009	02/14/06		Vulnerability in the Korean Input Method Editor Could Allow Elevation of Privilege (901190)	Not Applicable				
MS06-008	02/14/06	KB911927	Vulnerability in Web Client Service Could Allow Remote Code Execution (911927)	Not Applicable		SEC004S	SEC004S	√
MS06-007	02/14/06	KB913446	Vulnerability in TCP/IP Could Allow Denial of Service (913446). (Replaces MS05-019)	Not Applicable		SEC004S	SEC004S	√
MS06-006	02/14/06	KB911564	Vulnerability in Windows Media Player Plug-in with Non-Microsoft Internet Browsers Could Allow Remote Code Execution (911564)	Not Applicable		SEC004S	SEC004S	√
MS06-005	02/14/06	KB911565	Vulnerability in Windows Media Player Could Allow Remote Code Execution (911565). (Replaces MS05-009)	Not Applicable		Approved	Not Applicable	
MS06-004	02/14/06		Cumulative Security Update for Internet Explorer (910620)	Not Applicable				

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS06-003	01/10/06		Vulnerability in TNEF Decoding in Microsoft Outlook and Microsoft Exchange Could Allow Remote Code Execution (902412)	Not Applicable				
MS06-002	01/10/06		Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution (908519)	Approved	Approved	SEC004S	SEC004S	√
MS06-001	01/05/06	KB912919	Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution (912919)	SEC004S	Approved	SEC004S	SEC004S	√
MS05-055	12/13/05	KB908523	Vulnerability in Windows Kernel Could Allow Elevation of Privilege (908523)	Approved	Approved	Not Applicable		
MS05-054	12/13/05	KB905915	Cumulative Security Update for Internet Explorer (905915) (Replaces MS05-052)	Not Applicable		Approved	Approved	√
MS05-053	11/08/05		Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (896424)	SEC003S	SEC003S	SEC003S	SEC003S	√
MS05-052	10/11/05		Cumulative Security Update for Internet Explorer (896688) (Replaces MS05-038)	Not Applicable		SEC003S Superseded by MS05-054	SEC003S	Not Applicable
MS05-051	10/11/05	KB902400	Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)	Not Applicable		SEC003S	SEC003S	√
MS05-050	10/11/05		Vulnerability in DirectShow Could Allow Remote Code Execution (904706)	SEC003S	SEC003S	SEC003S	SEC003S	√
MS05-049	10/11/05		Vulnerabilities in Windows Shell Could Allow Remote Code Execution (900725). (Replaces MS05-016)	SEC003S	SEC003S	SEC003S	SEC003S	√
MS05-048	10/11/05		Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution (907245)	Not Applicable		SEC003S	SEC003S	√
MS05-047	10/11/05		Vulnerability in Plug and Play Could Allow Remote Code Execution and Local Elevation of Privilege (905749)	SEC003S	SEC003S	Not Applicable		
MS05-046	10/11/05	KB899589	Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589)	SEC003S	SEC003S	SEC003S	SEC003S	√
MS05-045	10/11/05	KB905414	Vulnerability in Network Connection Manager Could Allow Denial of Service (905414)	Not Applicable		SEC003S	SEC003S	√
MS05-044	10/11/05	KB905495	Vulnerability in the Windows FTP Client Could Allow File Transfer Location Tampering (905495)	Not Applicable		Approved	Not Applicable	
	08/09/05	KB898715	Update for Windows Installer 3.1 for Server 2003/SP1	Not Applicable		Approved	Approved	√
MS05-043	08/09/05		Vulnerability in Print Spooler Service Could Allow Remote Code Execution (896423)	SEC003S	SEC003S	Approved	Not Applicable	
MS05-042	08/09/05		Vulnerabilities in Kerberos Could Allow Denial of Service, Information Disclosure, and Spoofing (899587)	Not Applicable		SEC003S	SEC003S	√
MS05-041	08/09/05		Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (899591)	Not Applicable		SEC003S	SEC003S	√

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS05-040	08/09/05		Vulnerability in Telephony Service Could Allow Remote Code Execution (893756)	SEC003S	SEC003S	SEC003S	SEC003S	√
MS05-039	08/09/05		Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)	Approved	Approved	SEC003S	SEC003S	√
MS05-038	08/09/05		Cumulative Security Update for Internet Explorer (896727) (Replaces MS05-025)	Not Applicable		Approved	Approved	Not Applicable
						Superseded by MS05-052		
MS05-037	07/12/05	KB903235	Vulnerability in Jview Profiler Could Allow Remote Code Execution (903235)	Not Applicable		Approved, but not vulnerable by default	Approved, but not vulnerable by default	√
MS05-036	07/12/05	KB901214	Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (901214)	Not Applicable		SEC003S	SEC003S	√
MS05-035	07/12/05		Vulnerability in Microsoft Word Could Allow Remote Code Execution (903672)	Not Applicable				
MS05-034	06/14/05		Cumulative Service Update for ISA Server 2000 (899753)	Not Applicable				
MS05-033	06/15/05	KB896428	Vulnerability in Telnet Client Could Allow Information Disclosure (896428)	Not Applicable		SEC003S	SEC003S	√
MS05-032	06/14/05	KB890046	Vulnerability in Microsoft Agent Could Allow Spoofing (890046)	Not Applicable		SEC003S	SEC003S	√
MS05-031	06/15/05		Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution (898458)	SEC003S	SEC003S	Not Applicable		
MS05-030	06/14/05	KB897715	Cumulative Security Update in Outlook Express (897715)	Not Applicable		Approved, but not vulnerable by default	Not Applicable	
MS05-029	06/14/05		Vulnerability in Outlook Web Access for Exchange Server 5.5 Could Allow Cross-Site Scripting Attacks (895179)	Not Applicable				
MS05-028	06/14/05	KB896426	Vulnerability in Web Client Service Could Allow Remote Code Execution (896426)	Not Applicable		SEC003S	SEC003S	√
MS05-027	06/14/06		Vulnerability in Server Message Block Could Allow Remote Code Execution (896422)	SEC003S	SEC003S	SEC003S	SEC003S	√
MS05-026	06/14/05		Vulnerability in HTML Help Could Allow Remote Code Execution (896358). Replaces MS05-001.	SEC003S	SEC003S	SEC003S	SEC003S	√
MS05-025	06/15/05		Cumulative Security Update for Internet Explorer (883939). (Replaces MS05-020)	Not Applicable		Approved	Approved	√
						Superseded by MS05-038		√
MS05-024	05/10/05		Vulnerability in Web View Could Allow Remote Code Execution (894320)	Not Applicable				
MS05-023	04/12/05		Vulnerabilities in Microsoft Word May Lead to Remote Code Execution (890169)	Not Applicable				

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS05-022	04/12/05		Vulnerability in MSN Messenger Could Lead to Remote Code Execution (896597)	Not Applicable				
MS05-021	04/12/05		Vulnerability in Exchange Server 2003/2000 Could Allow Remote Code Execution (894549)	Not Applicable				
MS05-020	04/12/05		Cumulative Security Update for Internet Explorer (890923). (Replaces MS05-014)	Not Applicable		Superseded by MS05-025	Not Applicable	
MS05-019	04/12/05		Vulnerabilities in TCP/IP Could Allow Remote Code Execution and Denial of Service (893066)	SEC003S	SEC003S	Approved Superseded by MS06-007	Not Applicable	
MS05-018	04/12/05		Vulnerability in Windows Kernel Could Allow Elevation of Privilege and Denial of Service (890859)	SEC003S	SEC003S	Approved	Not Applicable	
MS05-017	04/12/05		Vulnerability in MSMQ Could Allow Remote Code Execution (892944)	SEC003S	SEC003S	Not Applicable		
MS05-016	04/12/05		Vulnerability in Windows Shell that Could Allow Remote Code Execution (893086)	SEC003S	SEC003S	Approved	Not Applicable	
				Superseded by MS05-049				
MS05-015	02/08/05		Vulnerability in Hyperlink Object Library Could Allow Remote Code Execution (888113)	SEC002S	SEC002S	SEC002S	√	√
MS05-014	02/08/05		Cumulative Security Update for Internet Explorer (867282) (Replaces MS04-038)	SEC002S	SEC002S	SEC002S	√	√
MS05-013	02/08/05		Vulnerability in the DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (891781)	SEC002S	SEC002S	SEC002S	√	√
MS05-012	02/08/05		Vulnerability in OLE and COM Could Allow Remote Code Execution (873333)	SEC002S	SEC002S	SEC002S	√	√
MS05-011	02/08/05		Vulnerability in Server Message Block Could Allow Remote Code Execution (885250)	SEC002S	SEC002S	SEC002S	√	√
MS05-010	02/08/05		Vulnerability in the License Logging Service Could Allow Code Execution (885834)	SEC002S	SEC002S	SEC002S	√	√
MS05-009	02/08/05		Vulnerability in PNG Processing Could Allow Remote Code Execution (890261)	Not Applicable		SEC002S	√	Not Applicable
						Superseded by MS06-005		
MS05-008	02/08/05		Vulnerability in Windows Shell Could Allow Remote Code Execution (890047)	Not Applicable		SEC002S	√	√
MS05-007	02/08/05		Vulnerability in Windows Could Allow Information Disclosure (888302)	Not Applicable				
MS05-006	02/08/05		Vulnerability in Windows SharePoint Services and SharePoint Team Services Could Allow Cross-Site Scripting and Spoofing Attacks (887981)	Not Applicable				
MS05-005	02/08/05		Vulnerability in Microsoft Office XP could allow Remote Code Execution (873352)	Not Applicable				
MS05-004	02/08/05		ASP.NET Path Validation Vulnerability (887219)	Not Applicable		SEC002S	√	√

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS05-003	01/11/05		Vulnerability in the Indexing Service Could Allow Remote Code Execution (871250)	Not Applicable		SEC002S	√	√
MS05-002	01/11/05		Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution (891711)	SEC002S	SEC002S	SEC002S	√	√
MS05-001	01/11/05		Vulnerability in HTML Help Could Allow Code Execution (890175)	SEC002S	SEC002S	SEC002S	Not Applicable	
				Superseded. Refer to MS05-026.				
MS04-045	12/14/04		Vulnerability in WINS Could Allow Remote Code Execution (870763).	SEC002S	SEC002S	SEC002S	√	√
MS04-044	12/14/04		Vulnerability in Windows Kernel and LSASS Could Allow Elevation of Privilege (885835).	SEC002S	SEC002S	SEC002S	√	√
MS04-043	12/14/04	KB873339	Vulnerability in HyperTerminal Could Allow Code Execution (873339)	SEC002S	SEC002S	SEC002S	√	√
MS04-042	12/14/04		Vulnerability in DHCP Could Allow Remote Code Execution and Denial of Service (885249)	SEC002S	SEC002S	Not Applicable		
MS04-041	12/14/04	KB885836	Vulnerability in WordPad Could Allow Code Execution (885836).	SEC002S	SEC002S	SEC002S	√	√
MS04-028 (Revised)	12/14/04		Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)	Not Applicable		√	√	√
MS04-039	11/09/04		Vulnerability in ISA Server 2000 and Proxy Server 2.0 Could Allow Internet Content Spoofing (888258)	Not Applicable				
MS04-038	10/12/04		Cumulative Security Update for Internet Explorer (834707). Replaces MS04-025.	Not Applicable		Approved, PAA-2004-0423-Global Superseded by MS05-014	Not Applicable	
MS04-037	10/12/04	KB841356	Vulnerability in Windows Shell Could Allow Remote Code Execution (841356). Replaces MS04-024.	SEC002S	SEC002S	SEC002S	Not Applicable	
MS04-036	10/12/04	KB883935	Vulnerability in NNTP Could Allow Remote Code Execution (883935)	SEC002S	SEC002S	SEC002S	Not Applicable	
MS04-035	10/12/04		Vulnerability in SMTP Could Allow Remote Code Execution (885881)	Not Applicable		SEC002S	Not Applicable	
MS04-034	10/12/04		Vulnerability in Compressed (zipped) Folders Could Allow Remote Code Execution (873376)	Not Applicable		SEC002S	Not Applicable	
MS04-033	10/12/04		Vulnerability in Microsoft Excel Could Allow Remote Code Execution (886836)	Not Applicable				
MS04-032	10/12/04	KB840987	Security Update for Microsoft Windows (840987). Replaces MS03-045.	SEC002S	SEC002S	SEC002S	Not Applicable	
MS04-031	10/12/04	KB841533	Vulnerability in NetDDE Could Allow Remote Code Execution (841533)	SEC002S	SEC002S	SEC002S	Not Applicable	
MS04-030	10/12/04		Vulnerability in WebDAV XML Message Handler Could Lead to a Denial of Service (824151)	Not Applicable		SEC002S	Not Applicable	

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS04-029	10/12/04	KB873350	Vulnerability in RPC Runtime Library Could Allow Information Disclosure and Denial of Service (873350). Replaces MS03-039.	SEC002S	SEC002S	Not Applicable		
MS04-028	09/14/04		Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)	Not Applicable, Reference PAA-2004-0370-Global		√	Not Applicable	
MS04-027	09/14/04		Vulnerability in WordPerfect Converter Could Allow Code Execution (884933)	Not Applicable, Reference PAA-2004-0370-Global			Not Applicable	
MS04-026	08/10/04		Vulnerability in Exchange Server 5.5 Outlook Web Access Could Allow Cross-Site Scripting and Spoofing Attacks (842436)	Not Applicable, Reference PAA-2004-0319-Global			Not Applicable	
MS04-025	07/30/04	KB867801	Cumulative Security Update for Internet Explorer (867801)	SEC001S or SEC002S	G082S or SEC002S	√	Not Applicable	
MS04-024	07/13/04	KB839645	Vulnerability in Windows Shell Could Allow Remote Code Execution (839645)	SEC001S Superseded by MS04-037. Reference PAA-2004-0423-Global	G082S	√	Not Applicable	
MS04-023	07/13/04	KB840315	Vulnerability in HTML Help Could Allow Code Execution (840315)	SEC001S or SEC002S	G082S or SEC002S	√	Not Applicable	
MS04-022	07/13/04		Vulnerability in Task Scheduler Could Allow Code Execution (841873)	Not Applicable, Reference PAA-2004-0282-Global				
MS04-021	07/13/04	KB841373	Security Update for IIS 4.0 (841373)	SEC001S or SEC002S	G082S or SEC002S	Not Applicable		
MS04-020	07/13/04	KB841872	Vulnerability in POSIX Could Allow Code Execution (841872)	SEC001S or SEC002S	G082S or SEC002S	Not Applicable		
MS04-019	07/13/04		Vulnerability in Utility Manager Could Allow Code Execution (842526)	Not Applicable, Reference PAA-2004-0282-Global			Not Applicable	
MS04-018	07/13/04		Cumulative Security Update for Outlook Express (823353)	Not Applicable, Reference PAA-2004-0282-Global		√	Not Applicable	
MS04-017	06/08/04		Vulnerability in Crystal Reports Web Viewer Could Allow Information Disclosure and Denial of Service (842689)	Not Applicable, Reference PAA-2004-0244-Global			Not Applicable	
MS04-016	06/08/04		Vulnerability in DirectPlay Could Allow a Denial of Service (839643)	Not Applicable, Reference PAA-2004-0244-Global		√	Not Applicable	
MS04-015	05/11/04		Vulnerability in Help and Support Center Could Allow Code Execution (840374)	Not Applicable		√	Not Applicable	
MS04-014	04/13/04	KB837001	Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution (837001)	SEC001S or SEC002S	G082S or SEC002S	√	Not Applicable	
MS04-013	04/13/04		Cumulative Security Update for Outlook Express (837009)	Not Applicable		√	Not Applicable	
MS04-012	04/13/04	KB828741	Cumulative Update for Microsoft RPC/DCOM (828741)	SEC001S or SEC002S	G082S or SEC002S	√	Not Applicable	
MS04-011	04/13/04	KB835732	Security Update for Microsoft Windows (835732)	SEC001S or SEC002S	G082S or SEC002S	√	Not Applicable	
MS03-046 (revised)	04/13/04		Vulnerability in Exchange Server Could Allow Arbitrary Code Execution	Not Applicable, Reference PAA-2004-0144-Global			Not Applicable	

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS02-011 (revised)	04/13/04		Authentication Flaw Could Allow Unauthorized Users to Authenticate to SMTP Service	Not Applicable, Reference PAA-2004-0144-Global			Not Applicable	
MS01-041 (revised)	04/13/04		Malformed RPC Request Can Cause Service Failure	Not Applicable, Reference PAA-2004-0144-Global			Not Applicable	
MS00-082 (revised)	04/13/04		Patch Available for "Malformed MIME Header" Vulnerability	Not Applicable, Reference PAA-2004-0095-Global			Not Applicable	
MS04-010	03/09/04		Vulnerability in MSN Messenger Could Allow Information Disclosure (838512)	Not Applicable, Reference PAA-2004-0095-Global			Not Applicable	
MS04-009	03/09/04		Vulnerability in Microsoft Outlook Could Allow Code Execution (828040)	Not Applicable, Reference PAA-2004-0095-Global			Not Applicable	
MS04-008	03/09/04		Vulnerability in Windows Media Services Could Allow a Denial of Service (832359)	Not Applicable, Reference PAA-2004-0095-Global			Not Applicable	
MS03-022 (revised)	03/09/04		Vulnerability in ISAPI Extension for Windows Media Services Could Cause Code Execution (822343)	Not Applicable, Reference PAA-2004-0095-Global			Not Applicable	
MS04-007	02/10/04	KB828028	An ASN.1 Vulnerability Could Allow Code Execution (828028) (Superseded by MS04-011.)	G070S Reference PAA-2004-0144-Global	G058S	√	Not Applicable	
MS04-006	02/10/04	KB830352	Vulnerability in the Windows Internet Naming Service (WINS) Could Allow Code Execution (830352)	G070S or SEC001S	G058S or G082S	√	Not Applicable	
MS04-005	02/10/04		Vulnerability in Virtual PC for MAC Could Lead To Privilege Elevation (835150)	Not Applicable, Reference PAA-2004-0049-Global			Not Applicable	
MS04-004	02/02/04	Q832894	Cumulative Security Update for Internet Explorer (832894). (Superseded by MS04-025.)	G070S Reference PAA-2004-0300-Global	G058S	√	Not Applicable	
MS04-003	01/13/04		Buffer Overrun in MDAC Function Could Allow Code Execution (832483)	G070S or SEC001S or SEC002S	G058S or G082S or SEC002S	√	Not Applicable	
MS04-002	01/13/04		Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation (832759)	Not Applicable, Reference PAA-2004-0008-Global			Not Applicable	
MS04-001	01/13/04		Vulnerability in ISA Server H.323 Filter Could Allow Remote Code Execution (816458)	Not Applicable, Reference PAA-2004-0008-Global			Not Applicable	
MS02-050 (revised)	11/12/03		Certificate Validation Flaw Could Enable Identify Spoofing (Q329115)	Not Applicable				
MS03-051	11/11/03		Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution (813360)	Not Applicable				
MS03-050	11/11/03		Vulnerabilities in Microsoft Word and Excel Could Allow Arbitrary Code to Run (831527)	Not Applicable				
MS03-049	11/11/03		Buffer Overrun in the Workstation Service Could Allow Code Execution (828749)	Not Applicable				
MS03-048	11/11/03	Q824145	Cumulative Patch for Internet Explorer (824145)	Superseded by MS04-004. Reference PAA-2004-0027-Global			Not Applicable	

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS03-047	10/15/03		Vulnerability in Exchange Server 5.5 Outlook Web Access Could Allow Cross-Site Scripting Attack (828489)	Not Applicable				
MS03-046	10/15/03		Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (829436)	Not Applicable				
MS03-045	10/15/03	KB824141	Buffer Overrun in the ListBox and in the ComboBox Control Could Allow Code Execution (824141)	G070S	G058S	√	Not Applicable	
				Superseded by MS04-011 Reference PAA-2004-0144-Global				
MS03-044	10/15/03	KB825119	Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (825119)	G050S or SEC001S or SEC002S	G014S or G082S or SEC002S	√	Not Applicable	
MS03-043	10/15/03	KB828035	Buffer Overrun in Messenger Service Could Allow Code Execution (828035)	G050S or SEC001S or SEC002S	G014S or G082S or SEC002S	√	Not Applicable	
MS03-042	10/15/03		Buffer Overrun in Windows Troubleshooter ActiveX Control Could Allow Code Execution (826232)	Not Applicable				
MS03-041	10/15/03	KB823182	Vulnerability in Authenticode Verification Could Allow Remote Code Execution (823182)	G050S	G014S	√	Not Applicable	
				Superseded by MS04-011. Reference PAA-2004-0144-Global				
MS03-040	10/03/03	Q828750, Q828026	Cumulative Patch for Internet Explorer, specifically Update for Windows Media Player Script Commands component (828026)	G050S or SEC001S or SEC002S	G014S or G082S or SEC002S	√	Not Applicable	
MS03-039	09/03/03	KB824146	Buffer Overrun in RPCSS Service Could Allow Code Execution (824146)	G046S or G050S	G014S	√	Not Applicable	
				Superseded by MS04-012 Reference PAA-2004-0144-Global				
MS03-038	09/03/03		Unchecked Buffer in Microsoft Access Snapshot Viewer Could Allow Code Execution (827104)	Not Applicable				
MS03-037	09/03/03	KB822150	Flow in Visual Basic for Applications Could Allow Arbitrary Code Execution (822715)	Not Applicable				
MS03-036	09/03/03		Buffer Overrun in WordPerfect Converter Could Allow Code Execution (827103)	Not Applicable				
MS03-035	09/03/03		Flaw in Microsoft Word Could Enable Macros to Run Automatically (827653)	Not Applicable				
MS03-034	09/03/03	KB824105	Flaw in NetBIOS Could Lead To Information Disclosure (824105)	G046S or G050S or SEC001S or SEC002S	G014S or G082S or SEC002S	√	Not Applicable	
MS03-033	08/20/03	Q823718	Unchecked Buffer in MDAC Function Could Enable System Compromise (Q823718)	G050S	G014S	Not Applicable		
MS03-032	08/20/03	Q822925	Cumulative Patch for Internet Explorer	Superseded by MS03-040		√	Not Applicable	

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS02-040 (revised)	08/20/03	See MS03-033	Unchecked Buffer in MDAC Function Could Enable System Compromise (Q326573)	Superseded by MS03-033		Not Applicable		
MS03-030 (revised)	08/20/03	Q819696i	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	G050S or SEC001S	G014S or G082S or SEC002S	√	Not Applicable	
MS03-029 (revised)	08/13/03	KB823803	Flaw in Windows Function Could Allow Denial of Service (823803)	G050S or SEC001S	G014S or G082S or SEC002S	Not Applicable		
MS03-031	07/23/03		Cumulative Patch for Microsoft SQL Server (815495)	Not Applicable				
MS03-030	07/23/03	Q819696i	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	G050S or SEC001S or SEC002S	G014S	Not Applicable		
				Revised				
MS03-029	07/23/03	Q823803i	Flaw in Windows Function Could Allow Denial of Service (823803)	G050S or SEC001S or SEC002S	G014S	Not Applicable		
				Revised				
MS03-028	07/16/03		Flaw in ISA Server Error Pages Could Allow Cross-Site Scripting Attack (816456)	Not Applicable				
MS03-027	07/16/03		Unchecked Buffer in Windows Shell Could Enable System Compromise (821557)	Not Applicable				
MS03-026	07/16/03	Q823980i	Buffer Overrun in RPC Interface Could Allow Code Execution (823980)	G039S or G046S or G050S	√	√	Not Applicable	Not Applicable
				Superseded by MS03-039 and MS04-012. Reference PAA-2004-0144-Global				
MS03-025	07/09/03		Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation (822679)	Not Applicable				
MS03-024	07/09/03	Q817606i	Buffer Overrun in Windows Could Lead to Data Corruption (817606)	G039S or G046S or G050S or SEC001S or SEC002S	SEC002S	Not Applicable		
MS03-023	07/09/03	Windows-KB823559-ENU	Buffer Overrun In HTML Converter Could Allow Code Execution (823559)	G039S or G046S or G050S or SEC001S or SEC002S	SEC002S	√	Not Applicable	

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS03-022	06/25/03		Flaw in ISAPI Extension for Windows Media Services Could Cause Code Execution (822343)	Not Applicable				
MS03-021	06/25/03		Flaw In Windows Media Player May Allow Media Library Access (819639)	Not Applicable				
MS03-020	06/04/03	Q818529	Cumulative Patch for Internet Explorer (818529)	G039S or G046S Superseded by MS03-032	√	Not Applicable		
MS03-019	05/28/03		Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service (817772)	Not Applicable				
MS03-018	05/28/03	Q11114i	Cumulative Patch for Internet Information Service (811114)	G039S or G046S or G050S or SEC001S or SEC002S	SEC002S	Not Applicable		
MS01-048 (revised)	05/17/03	Q305399i	Malformed Request to RPC EndPoint Mapper can Cause RPC Service to Fail	G039S or G046S or SEC001S or SEC002S Superseded by MS04-012. Reference PAA-2004-0144-Global	SEC002S	Not Applicable		
MS03-017	05/07/03		Flaw in Windows Media Player Skins Downloading could allow Code Execution (817787)	Not Applicable				
MS03-016	04/30/03		Cumulative Patch for Biztalk Server (815206)	Not Applicable				
MS03-015	04/23/03	Q813489	Cumulative Patch for Internet Explorer (813489)	G039S Superseded by MS03-020)	√	Not Applicable		
MS03-014	04/23/03		Cumulative Patch for Outlook Express (330994)	Not Applicable				
MS03-013	04/16/03	Q811493i	Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges (811493)	G039S or G046S or G050S or SEC001S Superseded by MS04-011. Reference PAA-2004-0144-Global	√	Not Applicable		
MS00-084 (revised)	06/23/03	Q278499i	Patch Available for 'Indexing Services Cross Site Scripting' Vulnerability	Not Applicable				
MS03-012	04/09/03		Flaw In Winsock Proxy Service And ISA Firewall Service Can Cause Denial Of Service (331066)	Not Applicable				

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS03-011	04/09/03	msjavwu	Flaw in Microsoft VM Could Enable System Compromise (816093)	G039S or G046S or G050S or SEC001S or SEC002S	SEC002S	Not Applicable		
MS03-010	03/26/03	None for NT 4.	Flaw in RPC Endpoint Mapper Could Allow Denial of Service Attacks (331953)	Need to Firewall Port 135		Not Applicable		
MS03-009	03/19/03		Flaw in ISA Server DNS Intrusion Detection Filter Can Cause Denial Of Service (331065)	Not Applicable				
MS03-008	03/19/03	js56men	Flaw in Windows Script Engine Could Allow Code Execution (814078)	G039S or G046S or G050S or SEC001S or SEC002S	SEC002S	Not Applicable		
MS03-007	03/17/03	Q815021i	Unchecked buffer in Windows component could cause web-server compromise (815021)	G039S or G046S or G050S or SEC001S or SEC002S	SEC002S	Not Applicable		
MS03-006	02/26/03		Flaw in Windows Me Help and Support Center Could Enable Code Execution (812709)	Not Applicable				
MS03-005	02/05/03		Unchecked Buffer in Windows Redirector Could Allow Privilege Elevation (810577)	Not Applicable				
MS03-004	02/05/03	Q810847	Cumulative Patch for Internet Explorer (810847)	G039S Superseded by MS03-020	√	Not Applicable		
MS03-003	01/22/03		Flaw in how Outlook 2002 handles V1 Exchange Server Security Certificates could lead to Information Disclosure (812262)	Not Applicable				
MS03-002	01/22/03		Cumulative Patch for Microsoft Content Management Server (810487)	Not Applicable				
MS03-001	01/22/03	Q810833i	Unchecked Buffer in Locator Service Could Lead to Code Execution (810833)	G039S or G046S or G050S or SEC001S or SEC002S	SEC002S	Not Applicable		
MS02-072	12/18/02		Unchecked Buffer in Windows Shell Could Enable System Compromise (329390)	Not Applicable				
MS02-071	12/11/02	Q328310i	Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation (328310)	G070S Superseded by MS04-011. Reference PAA-2004-0144-Global	G058S	Not Applicable		
MS02-070	12/11/02		Flaw in SMB Signing Could Enable Group Policy to be Modified (309376)	Not Applicable				

Microsoft Security Update Details				CallPilot Release				
Bulletin #	**Date**	**Hotfix**	**Description**	**2.02**	**2.5**	**3.0**	**4.0**	**5.0/5.1**
MS02-069	12/11/02	msjavwu	Flaw in Microsoft VM Could Enable System Compromise	√	√	Not Applicable		
MS02-068	12/04/02	Q324929	Cumulative Patch for Internet Explorer (Q324929)	√	√	Not Applicable		
MS02-067	12/04/02		E-mail Header Processing Flaw Could Cause Outlook 2002 to Fail (331866)	Not Applicable				
MS02-050 (revised)	07/24/03	Q329115i	Certificate Validation Flaw Could Enable Identity Spoofing (Q329115)	√ Superseded by MS04-011. Reference PAA-2004-0144-Global	√	Not Applicable		
MS02-066	11/20/02	Q328970	November 2002, Cumulative Patch for Internet Explorer (Q328970)	√	√	Not Applicable		
MS02-065	11/20/02	Q329414.exe	Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution (Q329414)	SEC001S or SEC002S	G082S or SEC002S	Not Applicable		
MS02-064	10/30/02	permission change on root folder	Windows 2000 Default Permissions Could Allow Trojan Horse Program (Q327522)	√	√	Not Applicable		
MS02-063	10/30/02		Unchecked Buffer in PPTP Implementation Could Enable Denial of Service Attacks (Q329834)	Not Applicable				
MS02-062	10/30/02	Q327696	Cumulative Patch for Internet Information Service (Q327696)	√	√	Not Applicable		
MS02-061	10/16/02		Elevation of Privilege in SQL Server Web Tasks (Q316333)	Not Applicable				
MS02-060	10/16/02		Flaw in Windows XP Help and Support Center Could Enable File Deletion (Q328940)	Not Applicable				
MS02-059	10/16/02		Flaw in Word Fields and Excel External Updates Could Lead to Information Disclosure (Q330008)	Not Applicable				
MS02-058	10/10/02		Unchecked Buffer in Outlook Express S/MIME Parsing Could Enable System Compromise (Q328676)	Not Applicable				
MS02-057	10/02/02		Flaw in Services for Unix 3.0 Interix SDK Could Allow Code Execution (Q329209)	Not Applicable				
MS02-056	10/02/02		Cumulative Patch for SQL Server (Q316333)	Not Applicable				
MS02-055	10/02/02	hhupd.exe	Unchecked Buffer in Windows Help Facility Could Enable Code Execution (Q323255)	G039S or G046S or G050S	√	Not Applicable		
MS02-054	10/02/02		Unchecked Buffer in File Decompression Functions Could Lead to Code Execution (Q329048)	Not Applicable				
MS02-053	09/25/02		Buffer Overrun in SmartHTML Interpreter Could Allow Code Execution (Q324096)	Not Applicable				
MS02-052	09/18/02	vm-sfix3	Flaw in Microsoft VM JDBC Classes Could Allow Code Execution (Q329077)	G039S or G046S	√	Not Applicable		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS02-051	09/18/02		Cryptographic Flaw in RDP Protocol can Lead to Information Disclosure (Q324380)	Not Applicable				
MS02-050	09/09/02	Q328145i	Certificate Validation Flaw Could Enable Identity Spoofing (Q328145)	G039S Superseded by MS04-011. Reference PAA-2004-0144-Global	√	Not Applicable		
MS02-049	09/04/02		Flaw Could Enable Web Page to Launch Visual FoxPro 6.0 Application Without Warning (Q326568)	Not Applicable				
MS02-048	08/28/02	Q323172i	Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (Q323172)	G039S	√	Not Applicable		
MS02-047	08/22/02	Q323759	Cumulative Patch for Internet Explorer	G039S	√	Not Applicable		
MS02-046	08/22/02		Buffer Overrun in TSAC ActiveX Control Could Allow Code Execution (Q327521)	Not Applicable				
MS02-045	08/22/02	Q326830i	Unchecked Buffer in Network Share Provider Can Lead to Denial of Service (Q326830)	G039S	√	Not Applicable		
MS02-044	08/21/02		Unsafe Functions in Office Web Components (Q328130)	Not Applicable				
MS02-043	08/15/02		Cumulative Patch for SQL Server (Q316333)	Not Applicable				
MS02-042	08/15/02		Flaw in Network Connection Manager Could Enable Privilege Elevation (Q326886)	Not Applicable				
MS02-041	08/07/02		Unchecked Buffer in Content Management Server Could Enable Server Compromise (Q326075)	Not Applicable				
MS02-040	07/31/02	Q323264	Unchecked Buffer in OpenRowset Updates (Q326573)	Superseded by MS03-033.			Not Applicable	
MS02-039	07/24/02		Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution (Q323875)	Not Applicable				
MS02-038	07/24/02		Unchecked Buffer in SQL Server 2000 Utilities Could Allow Code Execution (Q316333)	Not Applicable				
MS02-037	07/24/02		Server Response to SMTP Client EHLO Command Results in Buffer Overrun (Q326322)	Not Applicable				
MS02-036	07/24/02		Authentication Flaw in Microsoft Metadirectory Services Could Allow Privilege Elevation (Q317138)	Not Applicable				
MS02-035	07/10/02		SQL Server Installation Process May Leave Passwords on System (Q263968)	Not Applicable				
MS02-034	07/10/02		Cumulative Patch for SQL Server (Q316333)	Not Applicable				
MS02-033	06/26/02		Unchecked Buffer in Profile Service Could Allow Code Execution in Commerce Server (Q322273)	Not Applicable				
MS02-032	07/24/02	vm320920	Cumulative Patch for Windows Media Player (Q320920)	√	√	Not Applicable		

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS02-031	06/19/02		Cumulative Patches for Excel and Word for Windows (Q324458)	Not Applicable				
MS02-030	06/12/02		Unchecked Buffer in SQLXML Could Lead to Code Execution (Q321911)	Not Applicable				
MS02-029	07/02/02	Q318138i	Unchecked Buffer in Remote Access Service Phonebook Could Lead to Code Execution	√	√	Not Applicable		
MS02-028	07/01/02		Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise (Q321599)	See Note 2		Not Applicable		
MS02-027	06/14/02	Q323759	Unchecked Buffer in Gopher Protocol Handler Can Run Code of Attacker's Choice (Q323889)	√	√	Not Applicable		
MS02-026	06/06/02		Unchecked Buffer in ASP.NET Worker Process (Q322289)	Not Applicable				
MS02-025	05/29/02		Malformed Mail Attribute can Cause Exchange 2000 to Exhaust CPU Resources (Q320436)	Not Applicable				
MS02-024	05/22/02	Q320206i	Authentication Flaw in Windows Debugger can Lead to Elevated Privileges	√	√	Not Applicable		
MS02-023	05/15/02	Q321232	Cumulative Patch for Internet Explorer	√	√	Not Applicable		
MS02-022	05/08/02		Unchecked Buffer in MSN Chat Control Can Lead to Code Execution (Q321661)	Not Applicable				
MS02-021	04/25/02		E-mail Editor Flaw Could Lead to Script Execution on Reply or Forward (Q321804)	Not Applicable				
MS02-020	04/17/02		SQL Extended Procedure Functions Contain Unchecked Buffers (Q319507)	Not Applicable				
MS02-019	04/16/02		Unchecked Buffer in Internet Explorer and Office for Mac Can Cause Code to Execute (Q321309)	Not Applicable				
MS02-018	04/10/02	Q319733i	Cumulative Patch for Internet Information Services	√	√	Not Applicable		
MS02-017	04/04/02	Q312895i	Unchecked buffer in the Multiple UNC Provider Could Enable Code Execution (Q311967)	√	√	Not Applicable		
MS02-016	04/04/02		Opening Group Policy Files for Exclusive Read Blocks Policy Application (Q318593)	Not Applicable				
MS02-015	03/28/02		Cumulative Patch for Internet Explorer	Superseded by MS02-023.			Not Applicable	
MS02-014	03/07/02	Q313829i	Unchecked Buffer in Windows Shell Could Lead to Code Execution	√	√	Not Applicable		
MS02-013	03/04/02	msjavx86	Cumulative VM Update	Superseded by MS02-052.			Not Applicable	
MS02-012	02/27/02		Malformed Data Transfer Request can Cause Windows SMTP Service to Fail	Not Applicable				
MS02-011	02/27/02		Authentication Flaw Could Allow Unauthorized Users To Authenticate To SMTP Service	Not Applicable				
MS02-010	02/21/02		Unchecked Buffer in ISAPI Filter Could Allow Commerce Server Compromise	Not Applicable				

Microsoft Security Update Details				CallPilot Release				
Bulletin #	Date	Hotfix	Description	2.02	2.5	3.0	4.0	5.0/5.1
MS02-009	02/21/02	vbs55men	Incorrect VBScript Handling in IE can Allow Web Pages to Read Local Files	√	√	Not Applicable		
MS02-008	02/21/02		XMLHTTP Control Can Allow Access to Local Files	SEC001S or SEC002S	G082S or SEC002S	Not Applicable		
MS02-007	02/20/02		SQL Server Remote Data Source Function Contain Unchecked Buffers	Not Applicable				
MS02-006	02/12/02	Q314147i	Unchecked Buffer in SNMP Service Could Enable Arbitrary Code to be Run	√	√	Not Applicable		
MS02-005	02/11/02		Cumulative Patch for Internet Explorer	Superseded by MS02-023.			Not Applicable	
MS02-004	02/07/02		Unchecked Buffer in Telnet Server Could Lead to Arbitrary Code Execution	Not Applicable				
MS02-003	02/07/02		Exchange 2000 System Attendant Incorrectly Sets Remote Registry Permissions (Q316056)	Not Applicable				
MS02-002	02/06/02		Malformed Network Request can cause Office v.X for Mac to Fail (Q317879)	Not Applicable				
MS02-001	01/30/02	Within Q299444i	Trusting Domains Do Not Verify Domain Membership of SIDs in Authorization Data	√	√	Not Applicable		
MS01-056	11/20/01	WM 308567	Windows Media Player .ASF Processor Contains Unchecked Buffer	SEC001S or SEC002S	G014S or G082S or SEC002S	Not Applicable		
MS01-048	09/10/01	Q305399i	Malformed Request to RPC EndPoint Mapper can Cause RPC Service to Fail (Superseded by MS04-012)	√	√	Not Applicable		
MS01-044	01/29/01	frgvuli	File Fragment Reading via .HTR Vulnerability	√	√	Not Applicable		
MS01-029 (revised)	06/23/03	Q298598	Windows Media Player ,ASX Processor Contains Unchecked Buffer	G070S or SEC001S or SEC002S	G058S or G082S or SEC002S	Not Applicable		
MS01-022	04/18/01	rbupdate	WebDAV Service Provider Can Allow Scripts to Levy Requests As User	√	√	Not Applicable		
MS00-079	08/30/01	Q304158	HyperTerminal Buffer Overflow Vulnerability	√	√	Not Applicable		
MS99-041	09/30/99	fixrasi	RASMAN Security Descriptor Vulnerability	√	√	Not Applicable		
MS98-001	03/24/99		Disabling Creation of Local Groups On A Domain By Non-Administrative Users	√	√	Not Applicable		

Notes:

1. These security updates were tested and approved for directly downloading from Microsoft and installing on a CallPilot server.
2. HTR is disabled on CallPilot 2.0 and 2.02.
3. Application of MS07-012 requires the following additional step be taken AFTER rebooting the server.
    a. Using Windows Explorer, copy files **mfc40.dll** and **mfc40u.dll** from **C:\WINDOWS\system32** to **D:\Nortel\bin** (replacing the files in D:\Nortel\bin)
4. When installing MS08-008, it's highly recommended that KB946235 also be installed. It can be downloaded directly from: http://www.microsoft.com/downloads/details.aspx?FamilyID=C96420A9-7436-4625-9649-75F1514B0FE3&displaylang=en
5. When installing MS09-012, both updates are required.
6. If CPSECPEP011S has been previously installed, it implements a Microsoft-suggested workaround to disable the WordPerfect text converter. This means that CPSECPEP011S already protects against one of the four vulnerabilities addressed by MS09-010. However, because the workaround involves removing all permissions from the WordPerfect converter, it results in an error when MS09-010 installation is attempted. In order to get all four vulnerabilities fixed, we need to get the MS09-010 fully installed – therefore the following workaround needs to be carried out.
    a. **If CPSECPEP011S has been previously installed, prior to installing MS09-010**, at a command prompt type:
    cacls "%ProgramFiles%\Windows NT\Accessories\mswrd8.wpc" /E /P administrators:F everyone:F Users:F "power users":F "terminal server user":F
    b. Install MS09-010 either using Windows Update or the downloaded hotfix
    c. Reboot the server
    d. At a command prompt type:
    cacls "%ProgramFiles%\Windows NT\Accessories\mswrd8.wpc" /E /P administrators:N everyone:N Users:N "power users":N "terminal server user":N

    Note: This is automatically installed via security PEP CPSECPEP012S (and later).

7. MS10-034 introduces OS changes that will negatively impact My CallPilot operation, specifically download of the player. Ensure My CallPilot version 5.00.41.110 (and later) is applied to avoid this condition.

Appendix-B

The table below identifies the additional security-related enhancements that are available for CallPilot servers within CallPilot Server Security Update PEPs:

Description	CallPilot Release / PEP				
	2.02	2.5	3.0	4.0	5.0/5.1
Set Windows disk full warning threshold to 2%			SEC004S	SEC004S	SEC006S
Enable signatures on SMB			SEC004S	SEC004S	SEC006S
Disable updating of Last Access Time by NTFS			SEC004S	SEC004S	SEC006S
Set Event Log sizes, retention policy, and guest access			SEC004S	SEC004S	SEC006S
Remote Access Settings – disallow saving password, enable logging, answer after 5 rings, authentication retries 6, Time 2 min, Auto-disconnect 2 min, KeepConn 5 min			SEC004S	SEC004S	SEC006S
Set KeepAliveTime to 300,000ms according to MS recommendation			SEC004S	SEC004S	SEC006S
Disable AutoRun on all drives	SEC004S		SEC004S	SEC004S	SEC006S
Set ScreenSaver Grace Period to 0			SEC004S	SEC004S	SEC006S
Make proxy settings per-machine (Disallow per-user proxy settings)			SEC004S	SEC004S	SEC006S
Prevent Internet Explorer from automatically downloading new software to update/upgrade itself			SEC004S	SEC004S	SEC006S
Ensure that Software Update Shell Notifications are enabled			SEC004S	SEC004S	SEC006S
Tighten the handling of temporary directories used by Terminal Services (Remote Desktop) sessions			SEC004S	SEC004S	SEC006S
Remove Installer Policies Key to ensure that no elevated privileges have been given to the Installer			SEC004S	SEC004S	SEC006S
Although Posix subsystem disabled, removed an additional registry key associated with Posix	SEC004S		SEC004S	SEC004S	SEC006S
Tighten restrictions on Remote Desktop Connections			SEC012S	SEC012S	SEC012S
Prevent the installation of Microsoft Messenger Client			SEC012S	SEC012S	SEC012S
Disable PCHealth Error Reporting to Microsoft			SEC004S	SEC004S	SEC006S
Additional Internet Explorer hardening from DoD Gold Disk v2.0 Beta and Desktop Application STIG			SEC004S	SEC004S	SEC006S
Increased modem operation security	SEC002S	SEC002S	SEC002S	√	√
Additional hardening based on securws4 profile	SEC002S	SEC002S	SEC002S	SEC003S	√
Additional hardening based on Microsoft Windows Server 2003 Security Guide			SEC003S	SEC003S	√
Enable computer to stop generating 8.3 style filenames			SEC003S	SEC003S	√
Controls for # of additional Windows Socket connections to prevent DOS attacks			SEC003S	SEC003S	√
Disable auto-install of IE components			SEC003S	SEC003S	√
Ensure Software Update Shell Notifications are enabled			SEC003S	SEC004S	√
Terminal Services configured to not use Temp folders per Session and do not delete upon exit			SEC003S	SEC003S	√
Disable auto logon default password			SEC003S	SEC004S or SEC003S	√
Enable SaveDLLSearchMode			SEC003S	SEC003S	√
Disable Remote Desktop Sharing (as used by Microsoft conferencing products)			SEC003S	SEC003S	√
Use Only Machine Settings (not per user) for IE Security Zone Settings			SEC003S	SEC003S	√
Terminal Services – Set Time Limit for Disconnected Sessions and Disable Remote Assistance – Solicited Remote Assistance and Remote Assistance – Offer Remote Assistance			SEC003S	SEC003S	√
Windows Messenger – Do Not Allow Windows Messenger to be Run			SEC003S	SEC003S	√

Description	CallPilot Release / PEP				
	2.02	2.5	3.0	4.0	5.0/5.1
Enable Error Reporting – Report Errors			SEC003S	SEC003S	√
Disable Network Connections, Internet Connection Sharing, and Network Connections – Prohibit Install and Configuration of Network Bridge on the DNS Domain Network			SEC003S	SEC003S	√
Disallow Installation of Printers Using Kernel-mode Drivers			SEC003S	SEC003S	√
Media Player – Prevent Codec Download & Disable Auto-Update			SEC003S	SEC003S	√
Disable Messenger Client and Messenger Service software			SEC012S	SEC012S	SEC012S
Workaround for MS06-041: Modifying the Autodial DLL within Windows registry will prevent an application, specially crafted website or e-mail message from calling the affected API and exploiting the vulnerability.			SEC012S	SEC012S	SEC012S
Workaround for MS06-042: Disable caching of Web content in Internet Explorer			SEC012S	SEC012S	SEC012S
Control Access to data sources across domains (Local Zone and Trusted Sites Zone) (Internet Zone based on site being browsed)			SEC012S	SEC012S	SEC012S
Restricted Sites Zone- Ensure Active Scripting has level of protection based on site being accessed			SEC012S	SEC012S	SEC012S
Prevent execution of ActiveX controls not marked safe for scripting (prompt) (Local Zone, Internet Zone, Trusted Sites Zone)			SEC012S	SEC012S	SEC012S
Prevent execution of ActiveX controls not marked safe for scripting (Do not prompt)			SEC012S	SEC012S	SEC012S
Restricted Sites Zone- Ensure Allow META REFRESH has level of protection based on site being browsed			SEC012S	SEC012S	SEC012S
Ensure paste operations via script have level of protection based on site being accessed (Local Zone, Internet Zone, Trusted Sites Zone, and Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Ensure Display Mixed Content has level of protection based on site being browsed (Internet Zone, Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Ensure client certificates are not presented to web sites without the user’s acknowledgement (Local Zone, Internet Zone, Trusted Sites Zone, and Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Ensure Signed Active X controls cannot be downloaded (Internet Zone, Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Ensure Signed Active X controls cannot be downloaded without prompt (Local Zone, Trusted Sites Zone)			SEC012S	SEC012S	SEC012S
Ensure unsigned Active X controls cannot be downloaded (Local Zone, Internet Zone, Trusted Sites Zone, Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Ensure Drag and Drop (and copy/paste) of files has level of protection based on site being accessed (Internet Zone, Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Ensure IE Error Reporting is disabled since it could send sensitive info to vendor			SEC012S	SEC012S	SEC012S
Ensure file download is disabled (Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Prevent download of fonts (Restricted Sites Zone, Internet Zone- without prompt)			SEC012S	SEC012S	SEC012S
Ensure user is warned when changing zones			SEC012S	SEC012S	SEC012S
Ensure user is warned when IE form data is redirected to another site			SEC012S	SEC012S	SEC012S
			SEC012S	SEC012S	SEC012S
Ensure IE checks signatures on downloaded programs			SEC012S	SEC012S	SEC012S
Ensure IE warns of invalid certificates			SEC012S	SEC012S	SEC012S
Set to a custom level so other required settings can take effect (Local Zone, Restricted Sites Zone)			SEC012S	SEC012S	SEC012S

Description	CallPilot Release / PEP				
	2.02	2.5	3.0	4.0	5.0/5.1
Ensure Trusted Sites zone is set to custom level			SEC012S	SEC012S	SEC012S
Prevent execution of ActiveX controls not marked safe for scripting (Local Zone) (Internet Zone, Trusted, Sites Zone, and Restricted Sites Zone – set to prompt)			SEC012S	SEC012S	SEC012S
Prevent installation of desktop items (Internet Zone, Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Prevent installation of desktop items without a prompt (Local Zone, Trusted Sites Zone)			SEC012S	SEC012S	SEC012S
Set Java Permissions appropriate for Zone (Internet Zone, Trusted Zone, Restricted Sites Zone) (Local Zone – prompt)			SEC012S	SEC012S	SEC012S
Control Launching Programs and files in IFRAME (Local Zone, Internet Zone, Trusted Sites Zone, and Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Control Frames trying to navigate across different domains (Internet Zone, Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Control the running of ActiveX controls and plug-ins (Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Control the scripting of Java applets (Restricted Sites Zone) (Internet Zone- prompt)			SEC012S	SEC012S	SEC012S
Control Software Channel permissions (Local Zone, Internet Zone, Trusted Sites Zone, Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Control Submission of non-encrypted form data (Restricted Sites Zone) (Internet Zone – prompt)			SEC012S	SEC012S	SEC012S
User Authentication – Logon (control how credentials are passed to web sites) (Local Zone, Internet Zone, Trusted Sites Zone, Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Control user data persistence (Internet Zone, Restricted Sites Zone)			SEC012S	SEC012S	SEC012S
Enable Cipher setting for Triple DES 168/168, RC 2 128/128, RC4 128/128, and Skipjack for all protocols			SEC012S	SEC012S	SEC012S
Disable Cipher setting for NULL for all protocols			SEC012S	SEC012S	SEC012S
Enable MD5 and SHA Hashes for all protocols			SEC012S	SEC012S	SEC012S
Ensure IE SSL/TLS parameter allows SSL and TLS to be used from the browser			SEC012S	SEC012S	SEC012S
Disable Internet Printing Protocol			SEC012S	SEC012S	SEC012S
Set DCOM Static Allocation of Endpoints for NMAOS to ncacn_ip_tcp,0,5000 (always use port 5000)			SEC012S	SEC012S	SEC012S
Remove RunAs values in registry			SEC012S	SEC012S	SEC012S
MS06-067: Prevent the Microsoft DirectAnimation Path ActiveX control from running in Internet Explorer			SEC012S	SEC012S	SEC012S
MS07-011: Enable Embedded Object Blocking in Wordpad			SEC012S	SEC012S	SEC012S
MS07-020: (Microsoft animated help agent)			SEC012S	SEC012S	SEC012S
MS07-045: Set "kill bit" for certain COM objects			SEC012S	SEC012S	SEC012S
MS07-047: Disassociate the WMZ and WMD file extensions & Disassociation of WMZ and WMD in Windows prevents previewing or opening WMZ and WMD files in Windows Media Player.			SEC012S	SEC012S	SEC012S
MS07-056: remove news protocol handler to avoid Outlook news reader vulnerabilities			SEC012S	SEC012S	SEC012S
Disable SSLv2 since it is less secure and clients should be using SSLv3			SEC012S	SEC012S	SEC012S
Disable weak encryption algorithms (RC2 40bit; DES 56 bit; RC4 40bit; RC4 56bit; RC4 64bit)			SEC012S	SEC012S	SEC012S
MS08-008: Disable attempts to instantiate Microsoft Forms 2.0 ImageActiveX Control in IE			SEC012S	SEC012S	SEC012S
MS08-010: Disable COM object instantiation in IE			SEC012S	SEC012S	SEC012S
.NET disable running components signed or not-signed with Authenticode (Internet Zone)			SEC012S	SEC012S	SEC012S

Description	CallPilot Release / PEP				
	2.02	2.5	3.0	4.0	5.0/5.1
RealPlayer ActiveX vulnerability Workarounds: Set killbits for rmoc3260.dll version 6.0.10.45 (KB240797)			SEC012S	SEC012S	SEC012S
Close off unneeded TCP ports by using an IP Security policy (1027, 1031, 1033 and 2019)			SEC012S	SEC012S	SEC012S
Disable JavaScript in Adobe Reader PDF files for Administrator userid (workaround for multiple security vulnerabilities reported November 2008)			SEC012S	SEC012S	SEC012S
Improved disabling of the AutoRun on all drives			SEC012S	SEC012S	SEC012S
Uninstall unneeded Java Runtime Engine 1.3.1-11 from some CP Servers			SEC012S	SEC012S	SEC012S
Changed permissions on disabled services			SEC012S	SEC012S	SEC012S
Added more auditing to disabled services			SEC012S	SEC012S	SEC012S
Changed Audit Policy – Audit privilege use from Success&Fail to Failure only			SEC012S	SEC012S	SEC012S
Network Access Remotely accessible registry paths and subpaths			SEC012S	SEC012S	SEC012S
Network Security: LAN manager authentication level			SEC012S	SEC012S	SEC012S
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients			SEC012S	SEC012S	SEC012S
User Rights: Deny logon as a batch job			SEC012S	SEC012S	SEC012S
User Rights: Deny logon through Terminal Services			SEC012S	SEC012S	SEC012S
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers			SEC012S	SEC012S	SEC012S
System objects: Default owner for objects created by members of Administrators group			SEC012S	SEC012S	SEC012S
Remote Administration Service set to Disabled			SEC012S	SEC012S	SEC012S
Security Log: Maximum Event log size changed from 16384KB to 81920KB			SEC012S	SEC012S	SEC012S
MSS MinimumDynamicBacklog changed to 20 from 10			SEC012S	SEC012S	SEC012S
File Permissions tightened for several files			SEC012S	SEC012S	SEC012S
Autorun: HonorAutorun setting registry value set			SEC012S	SEC012S	SEC012S
IE hardening and zone settings updated			SEC012S	SEC012S	SEC012S
IIS6 Installation, several settings updated			SEC012S	SEC012S	SEC012S
Restrict permissions on some system tools			SEC012S	SEC012S	SEC012S
Audit failures for the Everyone group for all files/folders on the system drive			SEC012S	SEC012S	SEC012S
Set permissions for all DCOM objects to Administrators F, System F, Users R			SEC012S	SEC012S	SEC012S
Ensure policies are reprocessed even if Group Policy objects have not changed			SEC012S	SEC012S	SEC012S
Numerous services are set to disabled in order to reduce the attack surface			SEC012S	SEC012S	SEC012S
Logical Disk Manager (dmserver) service is set to manual in order to reduce the attack surface			SEC012S	SEC012S	SEC012S
Disable parsing of Quicktime files			SEC013S	SEC013S	SEC013S
Disallow anonymous SID/Name translation			SEC013S	SEC013S	SEC013S
Adobe Reader disallow opening non-PDF file attachments with external applications			SEC013S	SEC013S	SEC013S
Remove keys related to Remote Administration Service DCOM to fix event 10005 on reboot			SEC013S	SEC013S	SEC013S
Java JRE javaws vulnerability – set kill bit			SEC013S	SEC013S	SEC013S
Prevent Windows Media Player ActiveX control from running in IE (MS10-027 workaround)			SEC013S	SEC013S	SEC013S
Disable HCP protocol			SEC013S	SEC013S	SEC013S
Registry flag changes to protect against a security vulnerability in Macromedia Flash Player	SEC003S	SEC003S	SEC003S	SEC003S	√
Administrative shares no longer automatically created	G039S or G046S or G050S or SEC001S	SEC002S	√	√	√

Description	CallPilot Release / PEP				
	2.02	2.5	3.0	4.0	5.0/5.1
Permissions tightened on certain folders	G039S or G046S or G050S or SEC001S	SEC002S	√	√	√
Unneeded sample web content deleted	G039S or G046S or G050S or SEC001S	√	√	√	√
Installs MDAC 2.5/Service Pack 2 (needed to install MS03-033)	G050S	G014S			
Installs MDAC 2.5/Service Pack 3	SEC001S	G082S or SEC002S	√	√	√
Updated version of MSXML parser (4.0 SP2) is installed for new security update (hotfix) checker.	SEC001S	G082S or SEC002S			
Disables Messenger Service	G050S	G014S	√	SEC003S	√
Updates Server to Windows NT 4 Service Pack 6A	√	√			
Updates Internet Explorer to version 5.5 with Service Pack 2	√	√			
Converts the system drive (C or D, wherever Windows NT is located) to NTFS	√	√			
Converts default SNMP server start-up operation to "Disabled"	√	√	√	√	√
pcAnywhere 10.5.2 update applied to address Symantec pcAnywhere Service-Mode Help File Elevation of Privilege	G070S or SEC001S	G058S or G082S or SEC002S			
Microsoft C2 patch is applied (Knowledge Base article (KB244599)	G070S or SEC001S	G058S or G082S or SEC002S			
Patch for "This Certificate Has an Invalid Digital Signature" issue (KB305929)	SEC001S	G082S or SEC002S			
Patch for "Enabling the PIPE_CREATE_INSTANCE" flag for non-admin users" issue (KB823492)	SEC001S	G082S or SEC002S			
HTML Help update to limit functionality when it is invoked with the windows.showHelp() Method (KB811630)	SEC001S	SEC002S			
Disable ADODB.Stream on Internet Explorer (KB870669)	SEC001S	G082S or SEC002S	SEC002S	√	√
Newer version of URLSCAN (version 2.5) is installed with improved checking	SEC001S	G082S or SEC002S			
Latest version of MSI Installer is installed	SEC001S	G082S or SEC002S			
SLEE monitor support tool updated to provide support for Microsoft security updates MS02-071 and MS03-045	G070S or SEC001S	G058S or G082S or SEC002S			
Enabled logging for RAS communications	G070S or SEC001S	G058S or G082S or SEC002S	√	√	√
Enabled signing for SMB client and server	G070S or SEC001S	G058S or G082S or SEC002S	√	√	√
Disabled OS2 and Posix subsystems	G070S or SEC001S	G058S or G082S or SEC002S	√	SEC003S	√
Disabled CD-ROM auto-run	G070S or SEC001S	G058S or G082S or SEC002S	√	SEC003S	√
Enabled RAS NetBIOS auditing	G070S or SEC001S	G058S or G082S or SEC002S	√	√	√
Floppy drives are now only available to user's that are locally logged on	G070S or SEC001S	G058S or G082S or SEC002S	√	√	√

Description	CallPilot Release / PEP				
	2.02	2.5	3.0	4.0	5.0/5.1
Disabled RDS component of Internet Information Service (IIS)	G070S or SEC001S	G058S or G082S or SEC002S	√	√	√
Disabled Exec function of Server Side Includes on IIS	G070S or SEC001S	G058S or G082S or SEC002S	√	√	√
Tightened additional file and folder permissions	G070S or SEC001S	G058S or G082S or SEC002S	√	√	√
Unneeded web services are deleted or disabled	G070S or SEC001S	G058S or G082S or SEC002S	√	√	√
Additional services are set to disabled to reduce attack "surface". Refer to readme.txt file within PEP for specific services.	G070S or SEC001S	G058S or G082S or SEC002S	√	SEC003S	√

Appendix-C

The following provides information on how to verify installed Microsoft security updates (Hotfixes) on a Windows NT 4.0-based CallPilot server (Releases 2.02 and 2.5).

Microsoft has released a tool called "MBSAcli" to check a system to ensure that all relevant security updates are present. This tool replaces the "hfnetchk" tool that was available previously and does a better job of checking security updates for different OS components. A version of this "MBSAcli" tool is provided in the current PEPs within the \HotFixes\Checker folder (e.g. D:\TEMP\CP202SEC002S\HotFixes\Checker).

The tool makes use of an XML file from Microsoft called "mssecure_1033.cab" identifying which security updates are available, when they are needed and how to check for them. CallPilot "Server Security Update" PEPs contain the current "mssecure_1033.cab" file available at the time the PEP was created.

To run the security update (hotfix) checker:

1. Launch a command prompt window.
2. Navigate to the D:\TEMP\CP202SEC002S\HotFixes\Checker folder.
3. Run **CheckHotFixes.bat.**

Watch for "Patch Not Found" errors, which indicate security updates that are needed but are not installed. Ignore "Note" messages. These just provide some additional information related to a given patch.

Note: Prior to Security PEPs CP20127G070S (CallPilot 2.02) and CP25006G058S (CallPilot 2.5), it is normal for a warning to be shown related to MS02-055 and for MS03-045 to show Patch Not Found. Patches MS02-071 & MS03-045 caused a problem on CallPilot in previous security PEPs and were therefore not installed.

Note: The tool may give an error if the CallPilot server is still booting up. If this happens, run the tool again at a later time.

Note: For CP202SEC001S, it is normal for a warning to be shown related to MS01-041 since CallPilot has a more recent file version than expected.

To display a list of security updates (hotfixes) explicitly installed on this server:

1. Launch a command prompt window.
2. Navigate to the D:\TEMP\CP202SEC002S\HotFixes\Checker folder.
3. Run **ListHotFixes.bat**.

To run "MBSAcli" using a new input file downloaded from the Microsoft web site:

1. Launch a command prompt window.
2. Run **"mbsacli /hf"** for additional information on needed fixes.

Note: This may show some very recent security updates missing if more updates have been released since this PEP was released. DO NOT install additional security updates unless approved by Avaya. Check the Partner Information Center (PIC) website for the latest Product Advisory Alert (PAA) bulletins or contact your Avaya representative for assistance.

Appendix-D

The following provides information on how CheckHotFixes.bat (contained in CPSECPEP013S and later) can be utilized to check against the latest list of Microsoft hotfixes even if the CallPilot server does not have Internet access.

1. Download the latest version of **wsusscn2.cab** from a Microsoft web-site using a separate internet-connected PC.
    a. http://go.microsoft.com/fwlink/?LinkID=74689 or search using http://go.microsoft.com/fwlink/?LinkdID=76054 (Links are subject to change. If invalid, do an internet search (e.g. Google) for "**wsusscn2.cab**")
2. Copy the downloaded wsusscn2.cab file to the Checker folder on the CallPilot server.
    a. Open a Windows Explorer window
    b. Navigate to the Checker folder
        i. Path = D:\TEMP\CPSECPEP013S\Checker\
           Note: If the contents of D:\TEMP have been cleared out, run CPSECPEP013S.msi once again to create the directory and required contents. This will attempt to install all 105 MS hot fixes
    c. Rename the existing wsusscn2.cab to create a backup copy.
        i. Right-click wsusscn2.cab and enter new name such as "wsusscn2-orig.bat.
    d. Copy the downloaded wsusscn2.cab file from the network share, USB drive, or burned CD to the Checker folder on the CallPilot server hard drive.
        i. Right-click file wsusscn2.cab, drag it to the Checker folder, and select "**Copy Here**".
3. Open a command-prompt window, navigate to the checker folder, and run the batch file.
    a. Start > Run > CMD
    b. Change directories to the checker folder
        i. CD D:\TEMP\CPSECPEP013S\Checker
    c. Run the checkhotfixes.bat file
        i. Enter "**CheckHotFixes.bat**" and press **<Enter>**
4. Compare the results with approved security updates as noted in Appendix-A.

Appendix-E

The following outlines the processes for utilizing the Microsoft "Windows Update" utility for applying approved Microsoft Security Updates directly from Microsoft's web-site.

For CallPilot 3.0, 4.0, and 5.0/5.1 servers:

1. From the server console, click Start > All Programs > Windows Update.
2. If the web site says you need to update your Windows Update software, do so by following the instructions from the web site.
3. Select "Custom"
4. Click "Review and Install updates"
5. Carefully review each update listed, paying special attention to the Knowledge Base (KB) article number. Check the list of offered updates against the list in Appendix-A of this bulletin and uncheck any updates that are not authorized by this bulletin.
6. Once the list of updates contains only the desired, authorized updates, click "**Install Updates**".

IMPORTANT NOTES:

- **DO NOT** install SP1 on CallPilot 3.0 servers using Windows Update.
  - Only apply SP1 using PEP CP303SECSP1S.
- **DO NOT** install SP2 on CallPilot 3.0, 4.0, or 5.0 servers using Windows Update.
  - Only apply SP2 using PEP CPSECPEPSP2S
    - (Excluding 202i which has SP2 pre-installed).
  - On CallPilot 3.0 and 4.0 servers, PEP CPDSKPEP001S must be installed prior to installing CPSECPEPSP2S (SP2)
- **DO NOT** install Internet Explorer 7 or Internet Explorer 8 on the CallPilot server. IE 7 may however, be safely applied to the customer-provided web-server hosting CallPilot Manager/Reporter and/or My CallPilot.
  IE 8 support is pending and qualification is underway.

Additional "Tested and Approved" updates:

Hotfix	Description
KB110806	(5.0/High Availability Servers) Benefits of the Microsoft .NET Framework
KB890830	Windows Malicious Software Removal Tool – November 2012
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 SP2
KB922582	Error message when you try to update a Microsoft Windows-based computer: "0x80070002"
KB925336	FIX: Error message when you try to install a large Windows Installer package or a large Windows Installer patch package in Windows Server 2003 or in Windows XP: "Error 1718. File was rejected by digital signature policy"
KB925672	MS06-061: Security update for Microsoft XML Core Services 4.0 SP2
KB927891	Reliability update for an issue in the Windows Installer (MSI) that can affect performance during updates
KB927978	MS06-071: Security update for Microsoft XML Core Services 4.0

Hotfix	Description
KB928365	(5.0/High Availability Servers) Description of the security update for the .NET Framework 2.0 for Windows Server 2003
KB931836	February 2007 cumulative time zone update for Microsoft Windows operating systems. Must be used in conjunction with the associated CallPilot PEP: • CP303S02G07S (3.0 w/ Service Update 2) • CP404S02G56S (4.0 w/ Service Update 2) • CP404S03G23S (4.0 w/ Service Update 3)
KB933360	August 2007 cumulative time zone update for Microsoft Windows operating systems
KB936181	Security update for Microsoft XML Core Services 4.0 (additional fix for MS07-042)
KB936357	Fix for "Intel processor microcode issue"
KB942763	December 2007 cumulative time zone update for Microsoft Windows operating system (**NOTE:** An additional CallPilot PEP will be required to introduce the new time zone changes for Venezuela and Armenia only. Its availability is TBD at this time.)
KB942840	You may experience slow Web browser performance when you view a Web page that uses Jscript in Internet Explorer 6 on a Windows Server 2003-based computer or on a Windows XP-based computer
KB946235	Visual Basic 6.0 Service Pack 6 oleaut32.DLL Security Update
KB948496	An update to turn off default SNP features is available for Windows Server 2003-based and Small Business Server 2003-based computers. (**NOTE:** Only applies to systems with SP2 installed)
KB950582	Update to resolve an issue in which Autorun features were not correctly disabled
KB951847 KB959209	*** Required for 1005r and 1006r / High Availability systems *** .NET Framework 3.5/Service Pack 1 and .NET Framework 3.5 Family Update for .NET versions 2.0 through 3.5
KB953839	Cumulative security update for ActiveX (Killbits for Windows Server)
KB955759	Description of the AppCompat update for Indeo codec December 08, 2009
KB955839	December 2008 cumulative time zone update for Microsoft Windows Operating Systems
KB956391	Cumulative security update for ActiveX (Killbits for Windows Server)
KB960715	Update Rollup for ActiveX Kill Bits
KB967715	Update to resolve additional issue in which Autorun features were not correctly disabled
KB968389	Extended Protection for Authentication (credentials under certain scenarios)
KB969898	Update Rollup for ActiveX Kill Bits
KB970653	August 2009 cumulative time zone update for Microsoft Windows operating systems
KB971029	Update to the AutoPlay functionality in Windows
KB971737	Description of the update that implements Extended Protection for Authentication in Microsoft Windows HTTP Services (WinHTTP)
KB973686, KB973687, KB973688	When an application uses MSXML to process XHTML, redundant retrieval requests for well-known DTD files from the W3C Web server cause XHTML parsing to fail on a Windows-based computer
KB973917	Description of the update that implements Extended Protection for Authentication in Internet Information Services (IIS)
KB976098	December 2009 cumulative time zone update for Microsoft Windows operating systems
KB976749	Update for Internet Explorer 6 for Windows Server 2003 (if MS09-054 has been applied)
KB979306	February 2010 cumulative time zone update for Windows operating systems
KB981793	May 2010 cumulative time zone update for Windows operating systems
KB2158563	September 2010 cumulative time zone update for Windows operating systems
KB2345886	Description of the update that implements Extended Protection for Authentication in the Server service
KB2443685	December 2010 cumulative time zone update for Windows operating systems
KB2467659	Update for Internet Explorer for Windows Server 2003 (This update addresses an issue that is introduced by MS10-090)
KB2524375	Microsoft Security Advisory: Fraudulent Digital Certificates could allow spoofing
KB2562937	Microsoft Security Advisory: Update Rollup for Active X Kill Bits
KB2570791	August 2011 cumulative time zone update for Windows operating systems
KB2616676	Fraudulent Digital Certificates Could Allow Spoofing

Hotfix	Description
KB2633952	December 2011 cumulative time zone update for Windows operating systems
KB2647518	March 2012 cumulative security update for ActiveX Kill Bits
KB2661254	Microsoft Security Advisory: Update for minimum certificate key length
KB2695962	May 2012 Update rollup for ActiveX Kill Bits
KB2728973	Unauthorized Digital Certificates Could Allow Spoofing
KB2736233	Microsoft Security Advisory: Update Rollup for ActiveX Kill Bits: September 11, 2012
Macrovision	Microsoft Security Advisory 944653. Macrovision Vulnerability in Macrovision SECDRV.SYS Driver on Windows Could Allow Elevation of Privilege
KB2749655	Microsoft Security Advisory: Compatibility issues affecting signed Microsoft binaries
KB2756822	October 2012 cumulative time zone update for Windows operating systems

For CallPilot 2.02 and 2.5 servers:

1. From the server console, launch Internet Explorer and enter URL:
   http://windowsupdate.microsoft.com
2. Click "Product Updates".
3. Click "Critical Updates".
4. Click "Show individual updates".
5. Select the desired, approved security updates as outlined above.

Notes using Windows Update:

1. Install only those security updates associated with approved Knowledge Base articles as listed in Appendix-A of this bulletin (or other approved security updates as documented in Technical Security Advisory bulletins, Product Advisory Alerts, or other Product Bulletins).
2. CallPilot 3.0 servers MUST NOT install Service Pack 1 (SP1) using Windows Update. It can only be applied to a CallPilot server using PEP CP303SECSP1S.
3. CallPilot 2.02 or 2.5 servers MUST NOT install Internet Explorer 6/SP1 (IE6), IE7, IE8 or other non-critical updates that have not been approved for use with CallPilot.
4. For either CallPilot 2.02, 2.5, or 3.0 servers, it may be necessary to click "Yes" on a security warning asking if you want to install and run the Windows Update software from Microsoft. This software is approved for use on the CallPilot server and must be installed to utilize the Windows Update utility. Once installed, when running Windows Update a subsequent time, the warning message will not appear.
   a. On CallPilot 2.02 and 2.5 servers, this warning may appear after you click "Product Updates".
   b. On CallPilot 3.0and later servers, it may appear after you click on "Scan for updates".
5. When using Windows Update, depending on the updates selected/installed, a reboot may be required.

Prerequisite Notes:

1. Prior to installing any security update or CallPilot Security Update PEP, Avaya recommends that an appropriate system backup or RAID-split be performed.
2. Prior to installing the above updates, the following Security Update PEPs should first be applied.

CallPilot Server		Required PEP	Recommended Additional PEPs
Release	Build		
5.0	5.00.41.20		CPSECPEP014S
			CPSECPEPSP2S_v02
4.0	4.04.04.00		CPSECPEP014S
		CPDSKPEP001S	CPSECPEPSP2S_v02
3.0	3.03.06.02	CP303SECSP1S or CPSECPEPSP2S_v02	CPSECPEP014S
		CPDSKPEP001S	CP303SECSP2S_v02
2.5	2.50.06.14		CP250SEC003S
2.02	2.01.27.05		CP202SEC004S

Appendix-F

CallPilot server "low disk space" is a condition that may impact CallPilot server operation and performance. It may occur after applying Microsoft hotfixes, Security updates, or other PEPs/Service Updates (SUs). While most likely to occur on smaller 201i IPE systems, it may also be encountered on larger tower or rackmount platforms if not properly maintained. Symptoms vary depending on equipped features, but are most commonly reported as:

- CallPilot Manager / Unable to add new or modify users
- Desktop messaging / Fails to function

The following provides guidelines and recommended "Best Practice" actions for ensuring sufficient disk space (at least 10%) exists after applying Security updates or Microsoft hotfixes.

1. Install CPDSKPEP001S (CallPilot 3.0 and 4.0 systems only)
2. Delete hotfix uninstall folders C:\Windows\$NTUninstallKBnnnnnn$ (where nnnnnn is the Microsoft Knowledge Base article number).

   For example: C:\Windows\$NTUninstallKB913580$

   Note: Excludes folder KB931836 that must remain on the system.

3. Ensure any anti-virus applications are installed on D: drive rather than C: drive.
4. Compress C:\WINDOWS\hf_mig
5. Compress C:\WINDOWS\inf
6. Compress C:\WINDOWS\repair
7. Compress C:\WINDOWS\PCHEALTH
8. Compress C:\WINDOWS\Program Files
9. Compress C:\WINDOWS\i386
10. Delete large files from the desktop of any user (or move those files to D: drive.
11. Empty the Recycle Bin

Important Notes:

- Do not delete other files or folders as they may be needed for system operation.
- Do not compress any other files or folders
- Do not adjust the size of, or move the pagefile

The information in this document is subject to change without notice. Avaya reserves the right to make changes, without notice, in equipment design as engineering or manufacturing methods may warrant. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Avaya.