NORTEL NETWORKS
BUSINESS WITHOUT BOUNDARIES

Product Bulletin

Bulletin Number: P-2003-0277-Global-rev3
Date: 28 April 2004

CallPilot Server Security Update

Reason for Revision

This bulletin is being revised to reflect the latest updates with regards to Microsoft hotfixes as well as highlight the enhanced support for installing approved critical hotfixes directly from Microsoft.

Introduction

Nortel Networks is pleased to introduce comprehensive Server Security Update Product Enhancement Packages (PEPs) for use with CallPilot 1.07 and 2.x systems. Installation of these PEPs results in increased security of the CallPilot server by providing the applicable Microsoft hotfix updates as well as incorporating additional security-related enhancements.

This bulletin outlines the recommended actions specific to these PEP updates, information on how to obtain each, and in Appendix-A, a detailed confidential listing of what each includes. It also provides general information specific to Nortel Networks policy with regards to installing Microsoft hotfix updates on the CallPilot server.

CallPilot Policy for Microsoft Hotfixes

Background Information

- CallPilot uses a particular combination and specific versions of various Microsoft Windows Operating System (OS), web server, and browser components. Therefore, Nortel Networks does not install many security hotfixes 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.
- While most Microsoft hotfixes function properly on CallPilot, some hotfixes have been found to cause issues.
- Customers **should not** install non-Nortel-approved Microsoft hotfixes on the CallPilot server for the following reasons:

    - Customers may make mistakes in identifying which hotfixes are applicable to CallPilot and which exact version of a hotfix applies to CallPilot.
    - Microsoft hotfixes must be tested to ensure they do not impact CallPilot functionality prior to being installed on our customers' production servers.
    - If a customer alters the software or configuration of a CallPilot server in a manner not supported by Nortel Networks, future upgrades of CallPilot software could fail even though the system presently works fine. Nortel Networks testing is based on standard CallPilot configurations and cannot test all possible modifications of those configurations.

How Nortel Provides Microsoft hotfixes

- Each up-issue and release of CallPilot software incorporates the latest set of Microsoft security hotfixes available at the time the release or up-issue was built. In addition to new hotfixes, each software up-issue of CallPilot contains other security improvements that further harden CallPilot to attack.
- The latest software release contains incremental hotfixes and security enhancements over that of releases in Sustained/Retired status. Security-minded customers will therefore want to stay current with the latest release of CallPilot software.
- When Microsoft issues a new security hotfix, Nortel Networks evaluates whether it applies to CallPilot, its threat-severity, and its impact on CallPilot operation and stability. After successful testing, the hotfix is approved for direct download from Microsoft and installation on a CallPilot server.
    - Nortel will issue a Product Advisory Alert within two (2) business days of Microsoft notification advising whether the new security hotfix can be applied to CallPilot.
- All applicable Microsoft hotfixes will be made available via CallPilot "Server Security Update" PEPs that are targeted to be released on a quarterly basis for software releases with a "Current" 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.

Recommended Actions

Change Windows NT Passwords to Strong Values

An important component of CallPilot server security is with passwords. Windows NT 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 NT 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 PEP

The latest CallPilot Server Security Update PEP should be applied during the next maintenance activity. 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. Further, because each software issue contains security improvements, security-minded customers should upgrade to the current CallPilot release and apply the latest Security PEP to achieve the best protection.

CallPilot Server Security Update PEPs may contain Microsoft hotfixes that have already been manually applied to the server in response to a published Product Advisory Alert (PAA). In these scenarios, if one or more individual, approved hotfixes 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.

Server Security Update PEPs

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\CP20127G070S) 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 from five (5) to forty-five (45) minutes and may require multiple reboots.

The Server Security Update PEPs are as follows:

CallPilot Release	Build	PEP number	Hotfix Level	File size	Notes
2.5	2.50.06.14	CP20127G058S	MS04-007	13.4MB	4
		CP25006G014S	MS03-044	19.6MB	
2.02	2.01.27.05	CP20127G070S	MS04-007	13.4MB	4
		CP20127G050S	MS03-044	30.3MB	
		CP20127G046S	MS03-026, MS03-024, and MS03-039	27.5MB	Obsolete
		CP20127G039S	MS03-026	25.5MB	Obsolete
2.0	2.01.26.05	CP20126G091S	MS03-044	25.5MB	
		CP20126G090S	MS03-026, MS03-024, and MS03-039	27.5MB	Obsolete
		CP20126G082S	MS03-026	25.5MB	Obsolete
1.07	1.07.09.06	NM010709G104S	MS03-044	22.4MB	2, 3
		NM010709G102S	MS03-026, MS03-024, and MS03-039	23.4MB	Obsolete, Note 3
		NM010709G100S	MS03-026	21.9MB	Obsolete, Note 3
		NM010709G078S	MS02-023	107MB	1

Notes:

1. This PEP requires Service Update 4 (SU-04) be installed prior to installing this update.

2. This PEP requires Security Update PEP NM010709G078S be installed prior to installing this update. PEP NM010709G078S requires multiple automatic server reboots and takes approximately 45 minutes to install. Refer to Product Bulletin 2002-087 for details.

3. PEPs NM010709G100S and NM010709G102S are obsolete due to an issue identified within each when upgrading to CallPilot 2.x. If either PEP has been installed, ensure PEP NM010709G104S is installed prior to attempting an upgrade to 2.x. Reference PAA-2003-0330-Global for additional information.

4. This PEP requires the previous Server Security Update PEP be installed prior to installing this update.

Obtaining the PEP

"Server Security Update" PEPs, as with all CallPilot PEPs, are available for download from the Meridian PEP Library (MPL) website at: https://transportvo.nortelnetworks.com/mpl/mpl

Note: If you are new to the MPL website, you will need to register for a user ID/password. Please apply on-line at http://www.nortelnetworks.com or contact your Nortel Networks 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 1.07:

- NTP 555-7101-214: 200i Server Maintenance and Diagnostics
- NTP 555-7101-119: 201i Server Maintenance and Diagnostics
- NTP 555-7101-216: 702t Server Maintenance and Diagnostics
- NTP 555-7101-218: 1001rp Server Maintenance and Diagnostics
- General Release Bulletin GR-134: CallPilot 1.07
- Product Bulletin 2002-087: CallPilot 1.07 Server Security Update

CallPilot 2.0 and 2.02:

- 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

CallPilot 2.5:

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

All documents are available for download from the Partner Information Center (PIC) and Helmsman Express websites at the following URLs:

Partner Information Center	http://my.nortelnetworks.com
Helmsman Express CallPilot documentation	http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=documentation&tranProduct=8165

Appendix-A

The following table outlines specific Microsoft Security Bulletins and associated hotfixes that pertain to the Windows NT 4.0 Operating System (OS) and associated Microsoft components. For each Microsoft bulletin listed, it identifies whether or not it is applicable to CallPilot and if so, the corresponding release, PEP, or Service Update required for addressing the vulnerability.

Note: Only those Microsoft hotfixes 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 hotfixes should ever be installed.

Legend:
GnnnS - Server PEP number required to implement hotfix
SU-nn - Service Update required implementing the hotfix
N/A - The hotfix is Not Applicable to CallPilot and therefore is not required or installed
√ **-** The hotfix is incorporated into the base software release and no PEP is needed

Microsoft Hotfix Details				CallPilot Release / PEPs			
Bulletin #	**Date**	**Hotfix**	**Description**	**1.07**	**2.0**	**2.02**	**2.5**
MS04-014	04/13/04	KB837001	Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution (837001)	N/A	Approved, Reference Note 4 or PAA-2004-0144		
MS04-013	04/13/04		Cumulative Security Update for Outlook Express (837009)	Not Applicable			
MS04-012	04/13/04	KB828741	Cumulative Update for Microsoft RPC/DCOM (828741)	Approved, Reference PAA-2004-0144			
MS04-011	04/13/04	KB835732	Security Update for Microsoft Windows (835732)	Refer to Note 5	Approved, Reference PAA-2004-0144		
MS03-046 (revised)	04/13/04		Vulnerability in Exchange Server Could Allow Arbitrary Code Execution	Not Applicable			
MS02-011 (revised)	04/13/04		Authentication Flaw Could Allow Unauthorized Users to Authenticate to SMTP Service	Not Applicable			
MS01-041 (revised)	04/13/04		Malformed RPC Request Can Cause Service Failure	Not Applicable			
MS00-082 (revised)	04/13/04		Patch Available for "Malformed MIME Header" Vulnerability	Not Applicable			
MS04-010	03/09/04		Vulnerability in MSN Messenger Could Allow Information Disclosure (838512)	Not Applicable			
MS04-009	03/09/04		Vulnerability in Microsoft Outlook Could Allow Code Execution (828040)	Not Applicable			
MS04-008	03/09/04		Vulnerability in Windows Media Services Could Allow a Denial of Service (832359)	Not Applicable			
MS03-022 (revised)	03/09/04		Vulnerability in ISAPI Extension for Windows Media Services Could Cause Code Execution (822343)	Not Applicable			

Microsoft Hotfix Details				CallPilot Release / PEPs			
Bulletin #	**Date**	**Hotfix**	**Description**	**1.07**	**2.0**	**2.02**	**2.5**
MS04-007	02/10/04	KB828028	An ASN.1 Vulnerability Could Allow Code Execution (828028) (Superceded by MS04-011)	Reference PAA-2004-0144		G070S	G058S
				Superceded. Reference PAA-2004-0144			
MS04-006	02/10/04		Vulnerability in the Windows Internet Naming Service (WINS) Could Allow Code Execution (830352)	Reference PAA-2004-0049		G070S	G058S
MS04-005	02/10/04		Vulnerability in Virtual PC for MAC Could Lead To Privilege Elevation (835150)	Not Applicable			
MS04-004	02/02/04	Q832894	Cumulative Security Update for Internet Explorer (832894)	Reference PAA-2004-0027		G070S	G058S
MS04-003	01/13/04		Buffer Overrun in MDAC Function Could Allow Code Execution (832483)	N/A	PAA-2004-0008	G070S	G058S
MS04-002	01/13/04		Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation (832759)	Not Applicable			
MS04-001	01/13/04		Vulnerability in ISA Server H.323 Filter Could Allow Remote Code Execution (816458)	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) (Superceded by MS04-004)	Superceded. Reference PAA-2004-0027			
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) (Superceded by MS04-011)	See Note 2		G070S	G058S
				Superceded. Reference PAA-2004-0144			
MS03-044	10/15/03	KB825119	Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (825119)	G104S	G091S	G050S	G014S

Microsoft Hotfix Details				CallPilot Release / PEPs			
Bulletin #	**Date**	**Hotfix**	**Description**	**1.07**	**2.0**	**2.02**	**2.5**
MS03-043	10/15/03	KB828035	Buffer Overrun in Messenger Service Could Allow Code Execution (828035)	G104S	G091S	G050S	G014S
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) (Superceded by MS04-011)	G104S	G091S	G050S	G014S
				Superceded. Reference PAA-2004-0144			
MS03-040	10/03/03	Q828750, Q828026	Cumulative Patch for Internet Explorer (828750) (Superceded by MS03-048)	G104S	G091S	G050S	G014S
				Superceded			
MS03-039	09/03/03	KB824146	Buffer Overrun in RPCSS Service Could Allow Code Execution (824146) (Superceded by MS04-012)	G104S	G090S or G091S	G046S or G050S	G014S
				Superceded. Reference PAA-2004-0144			
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)	G104S	G090S or G091S	G046S or G050S	G014S
MS03-033	08/20/03	Q823718	Unchecked Buffer in MDAC Function Could Enable System Compromise (Q823718)	N/A	G091S	G050S	G014S
MS03-032	08/20/03	Q822925	Cumulative Patch for Internet Explorer (Superceded by MS03-040)	Superceded			
MS02-040 (revised)	08/20/03	See MS03-033	Unchecked Buffer in MDAC Function Could Enable System Compromise (Q326573)	N/A	Superceded		
MS03-030 (revised)	08/20/03	Q819696i	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	G104S	G091S	G050S	G014S
MS03-029 (revised)	08/13/03	KB823803	Flaw in Windows Function Could Allow Denial of Service (823803)	G104S	G091S	G050S	G014S
MS03-031	07/23/03		Cumulative Patch for Microsoft SQL Server (815495)	Not Applicable			

Microsoft Hotfix Details				CallPilot Release / PEPs			
Bulletin #	**Date**	**Hotfix**	**Description**	**1.07**	**2.0**	**2.02**	**2.5**
MS03-030	07/23/03	Q819696i	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	G104S	G091S	G050S	G014S
MS03-029	07/23/03	Q823803i	Flaw in Windows Function Could Allow Denial of Service (823803)	G104S	G091S	G050S	G014S
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) (Superceded by MS03-039 and MS04-012)	G104S	G082S or G090S or G091S	G039S or G046S or G050S	√
				Superceded. Reference PAA-2004-0144			
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)	G104S	G082S or G090S or G091S	G039S or G046S or G050S	√
MS03-023	07/09/03	Windows-KB823559-ENU	Buffer Overrun In HTML Converter Could Allow Code Execution (823559)	G104S	G082S or G090S or G091S	G039S or G046S or G050S	√
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) (Superceded by MS03-032)	G104S	G082S or G090S	G039S or G046S	√
				Superceded			
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)	N/A	G082S or G090S or G091S	G039S or G046S or G050S	√
MS01-048 (revised)	05/17/03	Q305399i	Malformed Request to RPC EndPoint Mapper can Cause RPC Service to Fail	G078S	G082S or G090S	G039S or G046S	√

Microsoft Hotfix Details				CallPilot Release / PEPs			
Bulletin #	**Date**	**Hotfix**	**Description**	**1.07**	**2.0**	**2.02**	**2.5**
			(Superceded by MS04-012)	Superceded. Reference PAA-2004-0144			
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) (Superceded by MS03-020)	MS03-020	G082S	G039S	√
					Superceded		
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) (Superceded by MS04-011)	G104S	G082S or G090S or G091S	G039S or G046S or G050S	√
				Superceded. Reference PAA-2004-0144			
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			
MS03-011	04/09/03	msjavwu	Flaw in Microsoft VM Could Enable System Compromise (816093)	G104S	G082S or G090S or G091S	G039S or G046S or G050S	√
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			
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)	G104S	G082S or G090S or G091S	G039S or G046S or G050S	√
MS03-007	03/17/03	Q815021i	Unchecked buffer in Windows component could cause web-server compromise (815021)	G104S	G082S or G090S or G091S	G039S or G046S or G050S	√
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			

Microsoft Hotfix Details				CallPilot Release / PEPs			
Bulletin #	**Date**	**Hotfix**	**Description**	**1.07**	**2.0**	**2.02**	**2.5**
MS03-004	02/05/03	Q810847, hhupd	Cumulative Patch for Internet Explorer (810847) (Superceded by MS03-020)	MS03-020	G082S or G090S	G039S	√
				Superceded			
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)	G104S	G082S or G090S or G091S	G039S or G046S or G050S	√
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) (Superceded by MS04-011)	See Note 2		G070S	G058S
				Superceded. Reference PAA-2004-0144			
MS02-070	12/11/02		Flaw in SMB Signing Could Enable Group Policy to be Modified (309376)	Not Applicable			
MS02-069	12/11/02	msjavwu	Flaw in Microsoft VM Could Enable System Compromise	G104S	G082S or G090S	√	√
MS02-068	12/04/02	Q324929	Cumulative Patch for Internet Explorer (Q324929)	G104S	G082S or G090S	√	√
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) (Superceded by MS04-011)	G104S	G082S or G090S	√	√
				Superceded. Reference PAA-2004-0144			
MS02-066	11/20/02	Q328970	November 2002, Cumulative Patch for Internet Explorer (Q328970)	G104S	G082S or G090S	√	√
MS02-065	11/20/02	Q329414.exe	Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution (Q329414)	G104S	G082S or G090S or G091S	√	√
MS02-064	10/30/02	permission change on root folder	Windows 2000 Default Permissions Could Allow Trojan Horse Program (Q327522)	N/A	G082S or G090S	√	√

Microsoft Hotfix Details				CallPilot Release / PEPs			
Bulletin #	**Date**	**Hotfix**	**Description**	**1.07**	**2.0**	**2.02**	**2.5**
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)	G104S	G082S or G090S	√	√
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)	G104S	G082S	G039S or G046S or G050S	√
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)	G104S	SU01 and G082S or G091S	G039S or G046S	√
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) (Superceded by MS04-011)	G104S	SU01 and G082S or G091S	G039S	√
				Superceded. Reference PAA-2004-0144			
MS02-049	09/04/02		Flaw Could Enable Web Page to Launch Visual FoxPro 6.0 Application Without Warning (Q326568)	Not Applicable			

Microsoft Hotfix Details				CallPilot Release / PEPs			
Bulletin #	**Date**	**Hotfix**	**Description**	**1.07**	**2.0**	**2.02**	**2.5**
MS02-048	08/28/02	Q323172i	Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (Q323172)	G104S	SU01 and G082S or G091S	G039S	√
MS02-047	08/22/02	Q323759	Cumulative Patch for Internet Explorer	G104S	SU01 and G082S	G039S	√
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)	G104S	SU01 and G082S or G091S	G039S	√
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) (Superceded by MS03-033)	N/A	Superceded		
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)	G104S	√	√	√

Microsoft Hotfix Details				CallPilot Release / PEPs			
Bulletin #	**Date**	**Hotfix**	**Description**	**1.07**	**2.0**	**2.02**	**2.5**
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	G104S	√	√	√
MS02-028	07/01/02		Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise (Q321599)	G104S	See Note 3		
MS02-027	06/14/02	Q323759	Unchecked Buffer in Gopher Protocol Handler Can Run Code of Attacker's Choice (Q323889)	N/A	SU01	√	√
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	G104S	√	√	√
MS02-023	05/15/02	Q321232	Cumulative Patch for Internet Explorer	G078S	√	√	√
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	G104S	√	√	√
MS02-017	04/04/02	Q312895i	Unchecked buffer in the Multiple UNC Provider Could Enable Code Execution (Q311967)	G078S	√	√	√
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 (Superceded by MS02-023)	Superceded			
MS02-014	03/07/02	Q313829i	Unchecked Buffer in Windows Shell Could Lead to Code Execution	G078S	√	√	√
MS02-013	03/04/02	msjavx86	Cumulative VM Update (Superceded by MS02-052)	G078S	Superceded		

Microsoft Hotfix Details				CallPilot Release / PEPs			
Bulletin #	**Date**	**Hotfix**	**Description**	**1.07**	**2.0**	**2.02**	**2.5**
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			
MS02-009	02/21/02	vbs55men	Incorrect VBScript Handling in IE can Allow Web Pages to Read Local Files	G078S	√	√	√
MS02-008	02/21/02		XMLHTTP Control Can Allow Access to Local Files	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	G078S	√	√	√
MS02-005	02/11/02		Cumulative Patch for Internet Explorer (Superceded by MS02-023)	Superceded			
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	G078S	√	√	√
MS01-056	11/20/01	WM 308567	Windows Media Player .ASF Processor Contains Unchecked Buffer	G078S	G091S	√	G014S
MS01-048	09/10/01	Q305399i	Malformed Request to RPC EndPoint Mapper can Cause RPC Service to Fail (Superceded by MS04-012)	G078S	√	√	√
				Superceded. Reference PAA-2004-0144			
MS01-044	01/29/01	frgvuli	File Fragment Reading via .HTR Vulnerability	G078S	√	√	√
MS01-029 (revised)	06/23/03	Q298598	Windows Media Player ,ASX Processor Contains Unchecked Buffer			G070S	G058S
MS01-022	04/18/01	rbupdate	WebDAV Service Provider Can Allow Scripts to Levy Requests As User	G078S	√	√	√
MS00-079	08/30/01	Q304158	HyperTerminal Buffer Overflow Vulnerability	G078S	√	√	√

Microsoft Hotfix Details				CallPilot Release / PEPs			
Bulletin #	**Date**	**Hotfix**	**Description**	**1.07**	**2.0**	**2.02**	**2.5**
MS99-041	09/30/99	fixrasi	RASMAN Security Descriptor Vulnerability	G078S	√	√	√
MS98-001	03/24/99		Disabling Creation of Local Groups On A Domain By Non-Administrative Users	G078S	√	√	√

Notes:

1. This hotfix has been tested and approved for directly downloading the hotfix from Microsoft's website and installing on a CallPilot server.

2. This hotfix was withdrawn from CallPilot 1.07 and 2.0 as it negatively impacts the server, impacting the functionality of the SLEE Monitoring diagnostic tool. The severity of this vulnerability is considered to be low. The SLEE tool was enhanced and this hotfix is now installed with CallPilot 2.02 PEP G070S and 2.5 PEP G058S.

3. HTR is disabled on CallPilot 2.0 and 2.02.

4. The vulnerability fixed in MS04-014 does not apply to CallPilot 1.07 servers as the Microsoft Jet Database Engine is not installed on this release. For CallPilot 2.02 and 2.5 servers, the vulnerability exists, is considered moderate, and application of the hotfix is supported provided the prerequisite Security PEPs have been applied.

5. Application of hotfix MS04-011 is supported on CallPilot 1.07 servers but requires manual steps be performed after application to allow CallPilot to function normally. Reference PAA-2004-0155-Global revision-2 for required supplemental information.

Appendix-B

The table below identifies the additional security-related enhancements that are available for CallPilot servers:

Description	CallPilot Release / PEP			
	1.07	2.0	2.02	2.5
Administrative shares no longer automatically created	G104S	G082S or G090S or G091S	G039S or G046S or G050S	√
Permissions tightened on certain folders	G104S	G082S or G090S or G091S	G039S or G046S or G050S	√
Unneeded sample web content deleted		G082S or G090S or G091S	G039S or G046S or G050S	√
Installs MDAC 2.5/Service Pack 2 (needed to install hotfix MS03-033)		G091S	G050S	G014S
Disables Messenger Service		G091S	G050S	G014S
Updates Server to Windows NT 4 Service Pack 6A	G078S	√	√	√
Updates Internet Explorer to version 5.5 with Service Pack 2	G078S	√	√	√
Converts the system drive (C or D, wherever Windows NT is located) to NTFS	G078S	√	√	√
Converts default SNMP server start-up operation to "Disabled"	G078S	√	√	√
pcAnywhere 10.5.2 update applied to address Symantec pcAnywhere Service-Mode Help File Elevation of Privilege			G070S	G058S
Microsoft C2 patch applied (Knowledge Base article KB244599)			G070S	G058S
SLEE monitor support tool updated to provide support for Microsoft hotfixes MS02-071 and MS03-045			G070S	G058S
Enabled logging for RAS communications			G070S	G058S
Enabled signing for SMB client and server			G070S	G058S
Disabled OS2 and Posix subsystems			G070S	G058S
Disabled CD-ROM auto-run			G070S	G058S
Enabled RAS NetBIOS auditing			G070S	G058S
CD-ROM and Floppy drives are now only available to user's that are locally logged on			G070S	G058S
Disabled RDS component of Internet Information Service (IIS)			G070S	G058S
Disabled Exec function of Server Side Includes on IIS			G070S	G058S
Tightened additional file and folder permissions			G070S	G058S
Unneeded web services are deleted or disabled			G070S	G058S
Additional services are set to disabled to reduce attack "surface": Alerter, License Logging Service, Messenger, Computer Browser, TCP/IP NetBIOS Helper, ClipBook Server, Directory Replicator, Net Logon, Schedule, TCP/IP Print Server, UPS			G070S	G058S

Appendix-C

Microsoft has released a tool called "hfnetchk" to check a system to ensure that all relevant security hotfixes are present. A version of this tool is provided in the PEP in the \HotFixes\Checker folder (e.g. D:\TEMP\CP20127G050S\HotFixes\Checker).

The tool makes use of an XML file from Microsoft called "mssecure.xml" identifying which hotfixes are available, when they are needed and how to check for them.

To run the hotfix checker:

1. Launch a command prompt window.
2. Navigate to the D:\TEMP\CP20127G050S\HotFixes\Checker folder.
3. Run **CheckHotFixes.bat.**

   Watch for "Patch Not Found" errors, which indicate hotfixes that are needed but are not installed.

   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.

To display a list of hotfixes explicitly installed on this server:

1. Launch a command prompt window.
2. Navigate to the D:\TEMP\CP20127G050S\HotFixes\Checker folder.
3. Run **ListHotFixes.bat**.

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

1. Launch a command prompt window.
2. Run **hfnetchk** with no additional parameters
   or
   Run **hfnetchk –v –z** for additional information on needed fixes.

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