NORTEL NETWORKS
BUSINESS WITHOUT BOUNDARIES

Product Advisory Alert

Bulletin Number: PAA-2004-0144-Global-rev2
Date: 30 April 2004

CallPilot Security Advisory: MS04-011 through MS04-014 (Revised)

Reason for re-issue

This bulletin is being re-issued to include supplemental information required when applying Microsoft hotfix MS04-011 on a CallPilot 1.07 server.

Problem Description

On April 13, 2004, Microsoft released security advisory bulletins MS04-011, MS04-012, MS04-013 and MS04-014 for newly discovered vulnerabilities within multiple Windows Operating System versions and associated components. Some of the vulnerabilities could allow an attacker to run arbitrary code on a CallPilot system, or lead to other system compromise.

As well, Microsoft released updated versions of hotfixes MS03-046, MS02-011, MS01-041, and MS00-082 but none of these updates apply to CallPilot.

Expected Severity

The following identifies each of these hotfixes and their expected severity as it pertains to CallPilot's usage of the Operating System and components:

Bulletin	Hotfix	Title	CallPilot Severity	CallPilot Status
MS04-014	KB837001	Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution (837001)	Moderate	Approved, Note 1
MS04-013		Cumulative Security Update for Outlook Express (837009)	Not Applicable	
MS04-012	KB828741	Cumulative Update for Microsoft RPC/DCOM (828741)	Low	Approved
MS04-011	KB835732	Security Update for Microsoft Windows (835732)	Critical	Approved, Note 2
MS03-046		Vulnerability in Exchange Server Could Allow Arbitrary Code Execution	Not Applicable	
MS02-011		Authentication Flaw Could Allow Unauthorized Users to Authenticate to SMTP Service	Not Applicable	
MS01-041		Malformed RPC Request Can Cause Service Failure	Not Applicable	
MS00-082		Patch Available for "Malformed MIME Header" Vulnerability	Not Applicable	

Notes:

1. 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.

2. The vulnerability fixed in MS04-011 (KB835732) can be applied to CallPilot 1.07 servers, but because it contains updates to hotfixes that weren't previously supported on CallPilot, additional manual steps are required to ensure CallPilot functions properly. Please refer to the "Recommended Action" section and "Appendix-A: Supplemental Instructions for CallPilot 1.07 servers" for additional details. No additional steps are required when applying this hotfix update to CallPilot 2.x servers.

Recommended Action

The vulnerabilities within the above hotfixes vary. While the severity levels of each range from low to critical, because one is viewed as critical, it is recommended that all of the applicable hotfixes above, especially MS04-011, be installed immediately provided the prerequisite Security PEPs have been installed.

When applying MS04-011 (KB835732), CallPilot 1.07 servers require additional steps be completed both when installing the hotfix update and also when performing ad-hoc or scheduled backups. Refer to Appendix-A for supplemental information.

CallPilot 2.x servers do not exhibit interaction problems with MS04-011 (KB835732) allowing the hotfix to be applied directly, or using Windows Update as noted below, without further interaction.

CallPilot 2.x offers greater security than earlier releases and ease of implementation for MS04-011 (KB835732) and other hotfixes. It is recommended that all security-conscious customers upgrade from 1.07 to 2.02 or 2.5 in order to take full advantage of these security benefits.

To apply MS04-011 directly from Microsoft's web site, the easiest way is to visit http://windowsupdate.microsoft.com. Click on "Product Updates". Under "Critical Updates", click "Show individual updates". Select "Security Update for Microsoft Windows (KB835732)".

Notes using Windows Update:

1. Install only the hotfixes associated with identified Knowledge Base articles as listed (or other approved hotfixes as documented in Product Advisory Alerts or Product Bulletin P-2003-0277-Global "CallPilot Server Security Update").

2. Do not install Internet Explorer 6 SP1 or other non-critical updates that have not been approved for use with CallPilot.

As an alternative to using Windows Update, each approved hotfix can be downloaded utilizing the Microsoft Security Bulletin links within the table above. Select and download the hotfix listed for Windows NT Server 4.0, Service Pack 6a.

Prerequisite Notes:

1. Prior to installing hotfixes MS04-011, MS04-012, or MS04-014 (2.x only) on a CallPilot server, the following CallPilot Security PEPs must be applied first.

CallPilot Server		Required PEP	Additional Required PEP
Release	Build		
2.5	2.50.06.14	CP25006G014S	CP25006G058S
2.02	2.01.27.05	CP20127G050S	CP20127G070S
2.0	2.01.26.05	CP20126G091S	N/A
1.07	1.07.09.06	NM010709G078S	NM010709G104S

2. Prior to installing any hotfix or Security Update PEP, Nortel Networks recommends that an appropriate system backup or RAID split be performed.

3. CallPilot 1.07 servers require additional steps be completed upon installing MS04-011. Refer to Appendix-A for additional information.

Expected Nortel Solution

CallPilot 1.07, 2.02, and 2.5 "Server Security Update" PEPs containing these hotfixes will be made available during the next "Service Update" (SU) interval.

Supplemental Documentation

Microsoft Security Bulletins discuss these issues in further detail. Click on the appropriate bulletin link in the table above or refer to the Microsoft Online Support web site.

References and Related Documents

Product Bulletin P-2003-0277-Global "CallPilot Server Security Update" will be updated to reflect the new hotfix status and PEP numbers as applicable. It will be available for download from the Partner Information Center (PIC) web site at http://my.nortelnetworks.com.

Appendix-A

Supplemental Instructions for CallPilot 1.07 Servers Only:

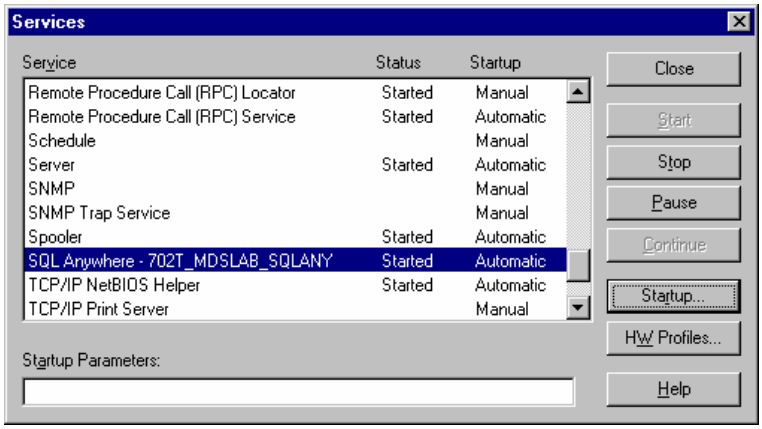
Hotfix MS04-011 (KB835732) contains updates to several hotfixes including MS02-071 and MS03-045 which were previously unsupported for use on CallPilot due to a negative impact to its operation. Because of this negative impact, and the critical nature of vulnerabilities addressed within MS04-011, it has been approved for application to the server but requires several additional steps be completed to overcome those identified interaction issues and ensure CallPilot functions properly.

After applying hotfix MS04-011 (KB835732) to a CallPilot 1.07 server, perform each of the following steps as necessary to ensure CallPilot functions properly.

1. This procedure is required for all CallPilot 1.07 servers after applying hotfix MS04-011.

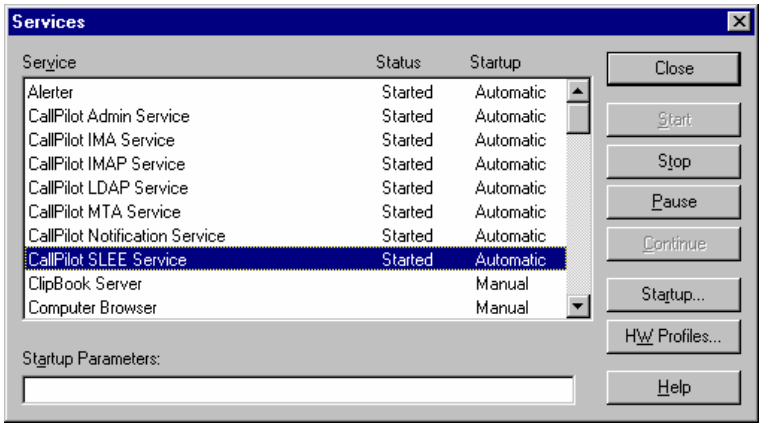
   Use Control Panel > Services to modify the startup parameters for the SQL Anywhere database service as follows:

   a. From the server console, launch Control Panel: Start > Settings > Control Panel.
   b. In Control Panel window, double-click "Services"
   c. In the "Services" window, select "SQL Anywhere" service and click "Startup"



   d. In the "Service" pop-up window, select "Allow Service to Interact with Desktop"

e. Click "OK" to close this window and return to the "Services" window.
f. In the "Services" window, select "CallPilot SLEE Service" and click "Startup"



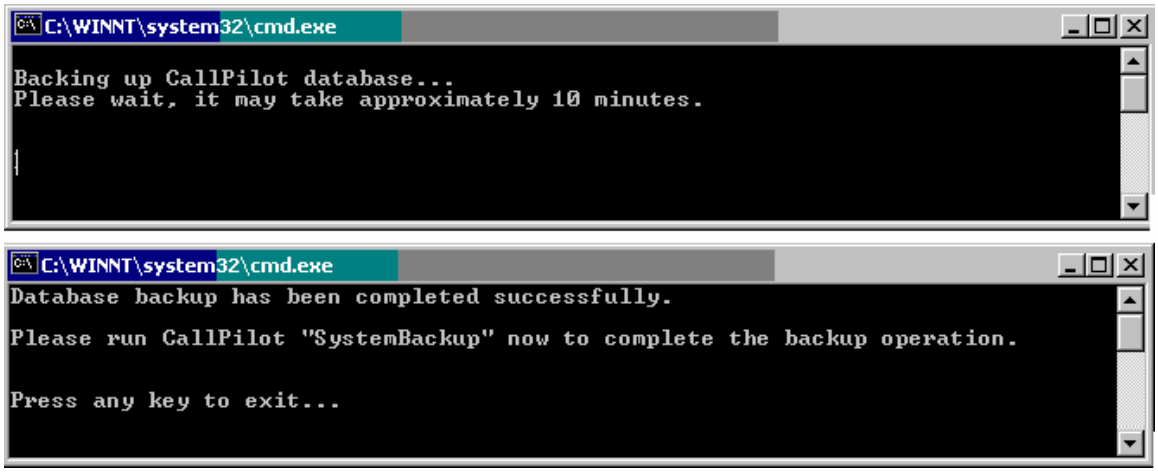
g. In the "Service" pop-up window, select "Allow Service to Interact with Desktop"

h. Close "OK" to close this window return to the "Services" window.
i. Click "Close" and exit from Control Panel
j. Reboot the server to full service, manually dismissing the pop-up window during the shutdown process.

Important Note: Upon reboot of CallPilot, a SQL Anywhere window will appear on the desktop. DO NOT close this window as it would impact CallPilot operation by stopping the SQLAnywhere service.

2. This procedure is **only required if system backups fail** with a "database file not found" error. It's recommended a backup be performed immediately after applying MS04-011 to test for this condition. (To check for backup errors, use the Admin Client – System Administration – Server Backup – Backup Manager to launch the "Backup History" window. Look at the completion status of the backup. If it says "some items skipped", you will need to use the workaround below. Also, in the Event Browser, Information Event 41881 will say that one or more items were skipped.)
   a. Obtain the files "DBBkp.exe" and "DBSnap.bat" from the Meridian PEP Library (MPL) website. (Both are posted under 1.07/Server PEP ID "DBBKP").

b. Copy or download "DBBkp.exe" and "DBSnap.bat" to the root folder of the D:\ drive. (You must use this location; otherwise modifications are required to the DBSnap batch file).
c. Launch a Command Prompt window using either of the two options:
    i. Start > Run > Enter "Cmd" in the Open window, click OK
    ii. Start > Programs > Command Prompt
d. Change directories to where the file was downloaded:
    i. e.g. "CD D:\"
e. Enter "DBBkp.EXE" and press <Enter>. The following windows will appear.

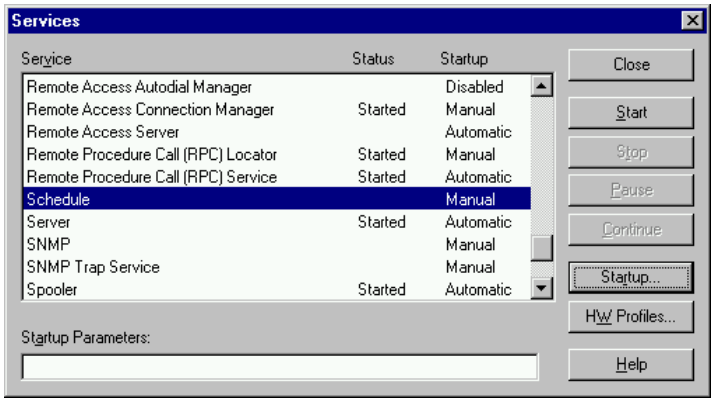


f. When complete, press any key to exit.
g. Type "Exit" to close the Command Prompt window.
h. Perform a CallPilot system backup as normal. It will pick up database files from the folder D:\Nortel\sysops\backup\database that have been created by DBBkp.exe

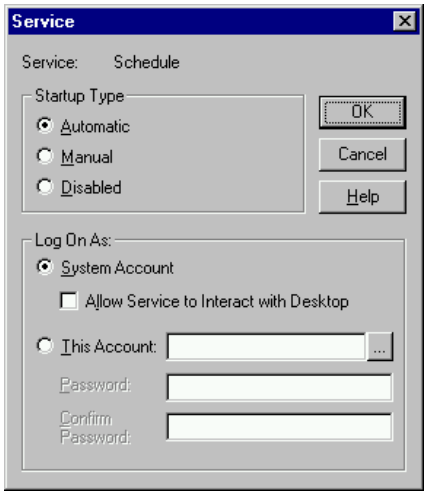
3. **This procedure is optional but highly recommended.** Using the Windows NT Scheduler, the "DBBkp.exe" utility can be scheduled to automatically run 15 minutes before a scheduled CallPilot backup. This allows the use of regularly scheduled backups without further user intervention.

   The example below shows the workaround used in conjunction with a scheduled CallPilot backup, occurring at 9:30pm every Friday evening.

   Use Control Panel > Services to modify the startup parameters for the Scheduler service as follows:
   a. From the server console, launch Control Panel: Start > Settings > Control Panel
   b. In Control Panel window, double-click "Services"
   c. In the "Services" window, select "Schedule" service and click "Startup"



d. In the "Service" pop-up window, change the Startup Type to "Automatic"



e. Close "OK" to close this window return to the "Services" window.
f. Click "Start" to start the Schedule service, and then "Close" to exit.
g. Close and exit from Control Panel
h. Launch a Command Prompt window using either of the two options:
    i. Start > Run > Enter "Cmd" in the Open window, click OK
    ii. Start > Programs > Command Prompt
i. If you plan to run a scheduled CallPilot backup every Friday at 9:30pm, at the D:\> prompt, type the following command:
    i. D:\> at 9:15pm /every:F d:\dbsnap.bat

Note: For details about the Windows "at" command, see the Windows NT on-line help using Start > Help. As well, using the "at" command with no parameter will display all scheduled commands.

Note: A GUI interface to the scheduler named "WinAT.exe" is available for download from http://www.dynawell.com. This is a more user-friendly version of the "at" command that may prove useful. You must still schedule the "DBSnap.bat" command even if you use WinAT.exe