NORTEL NETWORKS

*Product Bulletin*

Originator: C. Babin

Number: 2000-102

Date: November, 2000

# ADVISORY UPDATE

# Meridian 1 Security Alert

This bulletin is being issued as a follow up to Product Advisory 2000-085 - Meridian1 Security Alert.

## Problem Description:

In September, Nortel Networks was advised that the two diagnostic level passwords for Meridian 1 systems had been posted on an Internet chat room site. These passwords are considered by Nortel Networks to be company confidential and proprietary and are intended for use only by Nortel Networks technical support staff and our authorized distributors. These passwords apply to all Meridian 1 large machines running X11 Release 19 or later software and Option 11C with X11 Release 22 or later software. The diagnostic level passwords for these machines was hard coded and could not be changed at that time.

To reiterate our statement in September, Nortel Networks is not presently aware of any security incidents as a result of this information being posted. However we want our distributors and end customers to be fully aware of the situation and to know that we are continuing to take appropriate steps to ensure that access to their Meridian1 systems remains secure.

To this end, we are now announcing the availability of a patch that will allow an authorized Distributor or Nortel Networks Technician to change the diagnostic passwords. A patch is available for insertion into the systems and software issues listed below. The patch will allow the passwords to the diagnostic level of the M1 to be changed to a different set of characters.

## Expected Scope:

Any large Meridian 1 system running X11 Release 19 or later software and Option 11C running X11 Release 22 or later, will have these hard coded diagnostic level passwords. These systems may therefore be exposed to tampering by a knowledgeable person with either local or remote access to the maintenance port.

## Expected Solution:

Verification on the diagnostic level password patch for the first group of software issues and machine types has been completed. A patch for the listed machine types can be downloaded from the MPLR database for those distributors that are trained in system patching. For distributors that will not be doing their own patching, please contact CTS in order to schedule the loading of this patch. In order to minimize impact to the support provided by CTS on other technical issues, a team is being put in place specifically to insert this patch. CTS patching of the diagnostic level password change can be scheduled for insertion Monday through Friday during the hours of 8:00 am to 5:00 pm Central. If it is mandatory that the patch be inserted at another time, it can be discussed at time of scheduling.

## Recommended Action:

**ALTERNATE SECURITY:**

As stated in the first Meridian 1 Security Alert bulletin, Nortel still recommends that remote access to the PBX be restricted via a secure modem or use of a Virtual Private Network (VPN). As well, if the switch is accessible from a local LAN, then switch security can be achieved via standard network security methods.

If you choose to manage diagnostic level access security via the password, please adhere to the following.

**INTERACTIONS:**

Generally, MAT and OTM will not have any interaction issues with this patch. However, for the specific applications listed below, MAT and OTM communicate with the Meridian 1 system using the original hard coded diagnostic level access and password. Installing the diagnostic level password patch will result in the following limitations to the functionality of MAT and OTM.

1. **Scheduled CDR retrieval using Data Buffering and Access (DBA)**. If Data Buffering and Access is in use, CDR records will no longer be retrievable directly from the switch. An alternate method for MAT and OTM to collect CDR records from the switch is receive a real time feed of CDR records or to use an external buffer box that connects directly to the SDI port.
2. **MAT & OTM will be unable to download Corporate Directory** to the switch while this patch is in service. This will not affect the ability to create a Corporate Directory at the MAT/OTM level, nor the ability to export the directory to a spreadsheet. Also, this will not affect the ability of the M3900 set to use the Corporate Directory file within the switch.
3. **Inventory Reporting**. MAT/ OTM will no longer be able retrieve the Inventory file and therefore, to generate an inventory report.

If any of this functionality is mission critical to the site, the patch should not be installed and the alternate system security methods listed above should be used.

**NOTE** Our test results indicate that the applications listed above are the only ones impacted by the use of this patch. If a file retrieval action stops functioning after patch insertion, it may be due to this patch. Putting the patch out of service should return this functionality. At that point the alternate security methods will need to be utilized instead of the patch.

**PATCHING INSTRUCTIONS:**

It is very important that the patching instructions found on the patch database are followed precisely, in order to ensure that the diagnostic level passwords can be changed properly. Instructions can be found on the patching database.

Please note that the patching instructions have recently been updated to add a reference to case sensitivity when resetting the password. If you obtained it prior to November 3, 2000 it is recommended that you update your copy.

**PASSWORD MANAGEMENT AND RESET**

In the event that a password is forgotten or changed in error, diagnostic level can be entered via a physical reset method as described in the patching instructions. This will allow temporary access to the diagnostic level. The diagnostic level passwords can then be changed normally.

**NOTE** that it is the responsibility of the distributor to manage the diagnostic level passwords. In the event that a reset is required to be performed by CTS, distributor must have a person on site to invoke the reset.

## Fix Completion Date:

Patch creation is continuing and will be made available as soon as possible. Notification for the availability of these patches will be issued via product bulletin updates. It is expected that the patches will be made available in 2 groups:

CP2 to CP4 – Releases 22 and 23 / Option 11C 25.15

CP1 to CP4 – Release 19 and 21 as applicable / CP Pentium Release 25

**FUTURE ISSUES OF SOFTWARE**

This patch will be provided as a manufacture installed patch on Option 11C and on the MCDS disk for Release 25.30, so that it can be put into service or left out due to the MAT and OTM interaction.

We are currently investigating making the PDT password change capability permanent. In order to achieve this, the interactions with MAT and OTM will need to be resolved. The feasibility of making this available in the Release 26 timeframe is being assessed.

**AVAILABLE PEPS:**

The following is a list of software issues and machine types for which the PDT patch is currently available.

| PEP Id | Version | Machine | SW Load | Status |
|---|---|---|---|---|
| MPLR13326 | 2 | Meridian CP4 | 25.15 | Released |
| MPLR13326 | 3 | Meridian CP3 | 25.15 | Released |
| MPLR13326 | 4 | Meridian CP2 | 25.15 | Released |
| MPLR13326 | 5 | Meridian CP4 | 24.25 | Released |
| MPLR13326 | 6 | Meridian CP3 | 24.25 | Released |
| MPLR13326 | 7 | Meridian CP2 | 24.25 | Released |
| MPLR13326 | 8 | Option 11C | 24.24 | Released |
| MPLR13326 | 9 | Option 11C | 25.10 | Released |
| MPLR13326 | 10 | Meridian CP2 | 25.10 | Released |
| MPLR13326 | 11 | Meridian CP3 | 25.10 | Released |
| MPLR13326 | 12 | Meridian CP4 | 25.10 | Released |
| MPLR13326 | 13 | Option 11C | 25.08 | Released |
| MPLR13326 | 14 | Meridian CP2 | 25.08 | Released |
| MPLR13326 | 15 | Meridian CP3 | 25.08 | Released |
| MPLR13326 | 16 | Meridian CP4 | 25.08 | Released |
| MPLR13326 | 17 | Option 11C | 24.09 | Released |
| MPLR13326 | 18 | Option 11C | 23.55 | Released |
| MPLR13326 | 19 | Option 11C | 23.35 | Released |
| MPLR13326 | 20 | Option 11C | 23.18 | Released |
| MPLR13326 | 21 | Option 11C | 22.62 | Released |
| MPLR13326 | 22 | Option 11C | 22.46 | Released |
| MPLR13326 | 23 | Option 11C | 22.16 | Released |

## Documentation Forthcoming:

One or more further Product Advisory bulletin(s) will be issued, as the corrective patch is available for other software issues and machine types.