NORTEL

>TECHNICAL SUPPORT
TECHNICAL BULLETIN

Norstar and BCM: Preventative Measures for Toll Fraud

BULLETIN ID:	2009009392, Rev 1
PUBLISHED:	2009-03-18
STATUS:	Active
REGION:	APAC CALA EMEA GC NA
PRIORITY:	Critical
TYPE:	Alert

Background:

This bulletin identifies recommendations for Business Communications Manager (BCM) and Norstar product releases related to prevention of potential unauthorized malicious toll fraud.

The purpose of this document is to provide information on recommended programming and set up guidelines to avoid potential toll fraud issues on Norstar and BCM and their associated voicemail applications.

Before taking any action please ensure that you are viewing the latest official version of this bulletin checking on www.nortel.com and searching for this bulletin number.

Analysis:

Toll fraud occurs when unauthorized malicious users are able to access the central office facilities that are connected to the system for making outgoing calls. Norstar and BCM have several password and programming capabilities, from a system and user level, to aid in the security of the system which are outlined below.

The Norstar and BCM support a very rich set of security features and capabilities designed specifically to prevent such events. By observing recommended security practices, potential exposure can be avoided.

Although this document provides guidelines, it will not guarantee that all toll fraud issues will be eliminated; however, following these guidelines will certainly reduce the risk from unauthorized access and toll charges being incurred.

Recommendations:

Best practices that can be used in reducing potential toll fraud risk include the following:

1. Centralized Voicemail:

For sites that are not using Centralized Voicemail or Centralized Auto Attendant for multiple nodes, please ensure that the feature "Enable Network Transfers" is not checked. This option can be found under "Configuration" and "System Properties" within CallPilot Manager. "Enable Network Transfers" is unchecked by default.

On a site that is running centralized voicemail, "Enable Network Transfers" needs to be checked to allow functionality of the Centralized Auto Attendant. The feature "Enable Network Transfers" allows the Auto Attendant to route calls to routes

with the "Private" DN Type only (NOTE *1). Routes with any other DN Type are blocked, not allowing access to public Central Office facilities.

Recommendation: Only check "Enable Network Transfers" for a site using Centralized Voicemail to allow Centralized Auto-Attendant.

2. Passwords:

It is important to change all passwords on a regular basis. This includes the telephony configuration, administration, and voice mailbox passwords. This will prevent unauthorized access to the programming database where someone familiar with the system programming could potentially make changes which would allow them to access your lines to make long distance calls. Passwords chosen should not be Trivial and should never be left at default.

Recommendation: Passwords should not be left as default; change it as soon as the user account is setup and test/audit the change.

Recommendation: Change passwords frequently to meet company password policies.

Recommendation: Do not use trivial passwords.

3. Restrictions:

Restrictions provide the flexibility to add dialling restrictions to prevent specific area codes, telephone numbers, and long distance calls to be dialled. These restrictions can be programmed on a per set basis or per line basis. Restrictions can be overridden by COS (Class of Service) Passwords.

Recommendation: Add toll restrictions to those telephones that do not require the ability to make long distance calls.

Recommendation: If there is no requirement for Overseas Calling to be made, then all Lines should have a restriction filter for "011".

4. DISA (Direct Inward System Access)

DISA is a capability of the system to automatically answer a line and provide stuttered dial tone so that the caller can then dial an internal extension number or access an outside line to make a call. This feature is often used in situations where off-site employees need to make business long distance calls and have the calls billed directly to the company.

Lines answered with DISA and DISA DN provide stuttered dial tone which requires a COS (Class of Service) Password to be entered before any call can be made. Auto Answer and Auto DN give system dial tone and do not require any passwords to make a call. Auto Answer and Auto DN should NOT be used on public incoming lines.

Recommendation: Do not use Auto Answer and Auto DN on public incoming lines.

5. COS Password (Class of Service):

COS Passwords are user configured 6-digit passwords that are assigned to users and allow them to override restrictions assigned to telephones or lines, and allow access to DISA. COS passwords can also have restrictions enabled on what the user is allowed to dial.

Recommendation: COS Passwords should be complex numeric combinations, and not simple to guess. Do not use trivial passwords for COS passwords.

Recommendation: Restrictions should be applied to the COS password that will only allow calls that the user requires.

For example, if the user only needs to dial within a particular area code, then all other Long Distance for that password should be restricted.

6. External Call Forwarding:

The systems have an option called "Allow Redirect" which allows users to call forward their set to an external number. This option is disabled by default, and if not required, should not be changed to enabled for a user. The set's dialling restrictions also apply to the External Call Forward number.

Recommendation: Ensure "Allow Redirect" is set to "No" in set programming on telephones that should not have external call forward capability.

Recommendation: External Call Forwarding uses the set's restriction filter. Enabling set restrictions is another way to limit fraudulent usage.

7. Mailbox Outbound Transfer:

Outbound transfer from a mailbox is a feature that allows the user to set up another extension or external phone number in their mailbox that when a caller presses the access digit, the call will be transferred to that number. This option is Enabled/Disabled via the Mailbox Class of Service in CallPilot Manager programming and is enabled for many, but not all, of the default class of service. The mailbox programming must have "Outdial type" programmed for transferring to an external number. This option by default is set to "None", only allowing this feature to transfer to internal extensions.

Recommendation: This feature should only be enabled for users that require it.

Recommendation: Mailboxes are password protected and the passwords can be 4 to 8 digits in length. Mailbox user administration can be accessed off site. Choose a password that is not easy to guess. Do not use trivial passwords, for example "1111" or "1234". Choosing arbitrary digits for your passwords will increase the difficulty of unauthorized persons gaining access.

Recommendation: Enable Trivial password checking (NOTE *2) in CallPilot Manager.

Recommendation: Mailbox Class of Service should have passwords set to expire. Disabling password expiry increases the risk of unauthorized external access.

Recommendation: Outbound transfer uses the set's restriction filter. Enabling set restrictions is another way to limit fraudulent usage.

NOTE: This feature is not available on the older Norstar Startalk Flash and Startalk Mini.

8. Additional Measures:

In addition, there are other options available to assist in reducing toll fraud. Within the telephony configuration programming there is a feature called Restriction Service. Restriction Service can be set up so that toll restrictions to lines and telephone sets will automatically come on after business hours. This will prevent unauthorized personnel that have access to the business after hours and on weekends from using the telephones to make long distance calls. For example, if business hours are 8:00 a.m. until 6:00 p.m. Monday through Friday, the system can be programmed to automatically implement toll restriction on all telephones (or only selected telephones) from 6:00 p.m. to 8:00 a.m. Monday through Friday and from 6:00 p.m. Friday to 8:00 am Monday. Any employees who work during these off hours can still make a long distance call by entering their COS password as discussed earlier in this document. Line restrictions should be used to block any Long Distance areas that are not required to be dialled from the system and can be changed as business needs change.

Recommendation: Consider restricting long distance calls after business hours by using the Restriction Service feature.

Recommendation: Use Line Restrictions to block any Long Distance areas that are not required to be dialled from the system.

If there is suspicion of toll fraud activities, CDR (Call Detail Recording) can be used on the BCM to view a record all incoming and outgoing calls made from the system. For the Norstar System you will require an SMDR to collect the CDR Data.

Recommendation: Review CDR records regularly.

9. General Practices:

Nortel recommends that passwords of any kind for the system be changed on a regular basis to keep the integrity of the system secure. These passwords should be kept secure and only made available to the appropriate people that require that level of access. It is especially important to ensure that access passwords are changed any time someone leaves the company.

As usual, Nortel recommends:

- Customers create a company-wide security and virus protection policy for all elements of their network to reduce the threat of malicious attacks.

- Safeguarding your network to minimize the potential of future malicious exploitations, and the use of firewall rules for limiting access to known trusted endpoints to protect the systems and their associated voicemail application platforms.

- Any PC Clients connecting to the BCM, Norstar and their associated voicemail application platforms, have the necessary security updates installed.

Customers concerned about security, and customers with BCM, Norstar and their associated voicemail applications (NOTE * 3) systems containing earlier versions of software releases, should always consider upgrading to the latest release of software, using standard upgrade kits that are available through normal ordering process, to ensure they are taking advantage of the latest security measures incorporated into the product and in order to be ready to accept Patch Updates. Nortel strongly recommends upgrading to the latest release of software to reduce potential security exposures.

Safeguard your network by using firewall rules for limiting access to known trusted endpoints to protect the system.

Ensure that the system is updated with all currently available patches.

Although the implementation of the security recommendations and policies will continue to reduce the threat of future malicious attacks, the recommended programming configurations identified in this bulletin will help reduce the potential exploitation of the malicious toll fraud threats.

Contact regular technical support for any other technical issues related to this bulletin.

NOTES:

NOTE *1 - CallPilot 100/150 Software Version 2.10.08.00 and later, BCM 3.7 and later, and Norstar Voicemail Version 4.1 (NVM) with Patches (NVM_Toll_Fraud_CAA.exe or NVM_Toll_Fraud_Non-CAA.exe)

NOTE *2 - Option not available on the CallPilot 100/150 and Norstar Voicemail.

NOTE *3 - BCM and Norstar voicemail applications include CallPilot 100, CallPilot 150 and Norstar Voicemail

Required Actions:

See Recommendations.

Attachments:

There are no attachments for this bulletin

Footer Information:

For Additional Information:

Please contact your next level of support or visit <http://www.nortel.com/contact> for support numbers within your region. Channel Partners can access Nortel's Partner Information Center (PIC) website at <http://www.nortel.com/pic> , the Nortel Technical Support website at <http://www.nortel.com/support>, the Security Advisory Bulletins website at <http://www.nortel.com/securityadvisories> , and Nortel's Voice Security blog at <http://blogs.nortel.com/voicesecurity> .

Products and Releases:

The information in this bulletin is intended to be used with the following products and associated releases:

PRODUCT	RELEASE
BCM-BCM-BCM200 Global	
BCM-BCM-BCM200 N.A.	
BCM-BCM-BCM400 Global	
BCM-BCM-BCM400 N.A.	
BCM-BCM-BCM450 R1	
BCM-BCM-BCM50 Global	
BCM-BCM-BCM50 N.A.	
BCM-BCM-BCM50 R2 Global	
BCM-BCM-BCM50 R2 N.A.	
BCM-BCM-BCM50 R3 Global	
BCM-BCM-BCM50 R3 N.A.	
BCM-BCM-BCM50a Global	
BCM-BCM-BCM50a N.A.	
BCM-BCM-BCM50a R2 Global	
BCM-BCM-BCM50a R2 N.A.	
BCM-BCM-BCM50a R3 Global	
BCM-BCM-BCM50a R3 N.A.	
BCM-BCM-BCM50b R2 Global	
BCM-BCM-BCM50b R3 Global	
BCM-BCM-BCM50ba R2 Global	
BCM-BCM-BCM50ba R3 Global	
BCM-BCM-BCM50be R2 Global	

BCM-BCM-BCM50be R3 Global	
BCM-BCM-BCM50e Global	
BCM-BCM-BCM50e N.A.	
BCM-BCM-BCM50e R2 Global	
BCM-BCM-BCM50e R2 N.A.	
BCM-BCM-BCM50e R3 Global	
BCM-BCM-BCM50e R3 N.A.	
BCM-BCM-SRG200 1.0 Global	
BCM-BCM-SRG200 1.0 N.A.	
BCM-BCM-SRG200 1.5 Global	
BCM-BCM-SRG200 1.5 N.A.	
BCM-BCM-SRG400 1.0 Global	
BCM-BCM-SRG400 1.0 N.A.	
BCM-BCM-SRG400 1.5 Global	
BCM-BCM-SRG400 1.5 N.A.	
BCM-BCM-SRG50 2.0 Global	
BCM-BCM-SRG50 2.0 N.A.	
BCM-BCM-SRG50 3.0 Global	
BCM-BCM-SRG50 3.0 N.A.	
BCM-BCM-SRG50 Global	
BCM-BCM-SRG50 N.A.	
BCM-BCM-SRG50b 2.0 Global	
BCM-BCM-SRG50b 3.0 Global	
Norstar-Core-3X8	
Norstar-Core-CICS	
Norstar-Core-MICS	
Norstar-CallPilot-Norstar CallPilot 100	
Norstar-CallPilot-Norstar CallPilot 150	

To view the most recent version of this bulletin, access technical documentation, search our knowledge base, or to contact a Technical Support Representative, please visit Nortel Technical Support on the web at: http://support.nortel.com/. You may also sign up to receive automatic email alerts when new bulletins are published.

REFERENCE:
PRE-REQUIRED PATCH:
PATCH ID:

Nortel recommends any maintenance activities, such as those outlined in this bulletin, be completed during a local maintenance window.