

from Windows NT Embedded to Linux. The introduction of the BCM 4.0 and SRG200/400 RIs 1.5 software releases allows customers time to migrate the balance of the BCM and SRG portfolio to Linux through a software upgrade, thereby benefiting from the new Linux operating system, superior management capabilities, enhanced VoIP features and extensive security benefits.

ANALYSIS

Support Implications after December 31, 2006

Nortel will continue to support BCM 3.x and SRG 1.0 releases of software according to standard support policies in place at the time. Customers should expect no change in how Nortel supports the BCM product.

The only exception would relate to Nortel's ability to respond to potential Microsoft Windows NT Embedded security vulnerabilities that may occur after December 31, 2006. This is due to Microsoft's end of support policy. Consequently, BCM and SRG 1.0 systems running on this operating system cannot be patched to defend against any new Microsoft vulnerabilities discovered after that time.

It should be noted that while Windows NT based systems may become vulnerable to new forms of attack, this does not mean that 'malware' will attack a BCM system. The BCM uses a special version of Windows NT Embedded and has proven very resilient in avoiding security exposures over the past several years. In fact, only a very small number of Microsoft vulnerability exposures in the past, have required the creation of security patches for the BCM.

Other Considerations for Non-Upgraded Systems after December 31, 2006

By observing good security practices, the risk of a system being exposed to an attack to which it is potentially vulnerable can be reduced.

Examples of good security practices are:

- Create a company-wide security and virus protection policy for all elements of the network to reduce the threat of malicious attacks.
- Safeguard your network to minimize the potential of future malicious exploitations by using the built-in firewall rules for limiting access to known trusted endpoints to protect the BCM.
- Ensure a company access policy for the BCM, using BCM privileges to permit authorized access to the BCM.
- Implement a strong Password policy and change passwords to strong values.
- Using an anti-virus application on a secure Client PC, with up-to-date definitions, regularly perform anti-virus scans on BCM hard-drive drives.
- Do not map remote disks to the BCM Call Server.
- Do not map the BCM Call Server hard drives onto another server.

Customers should refer to the BCM Security Guide, located on the Partner Information Center, for further BCM security information.

RECOMMENDATIONS

BCM 4.0 - Industry Leading Converged System Security Capability

For customers concerned about the specific item of Microsoft security vulnerabilities, Nortel strongly recommends upgrading to the BCM 4.0 or SRG200/400 RIs 1.5 software release prior to January 1, 2007. This will ensure protection from any potential new Windows NT Embedded

vulnerabilities discovered after December 31, 2006.

Security conscious customers will benefit from a wide array of additional security enhancements included in the BCM 4.0 software release. Security remains a critical concern for customers, especially those leveraging IP networking to deliver business services. With the growing trend to convergence and VoIP, this concern is becoming even more critical.

To address this growing concern, the BCM portfolio is introducing a comprehensive series of security enhancements. These capabilities were introduced with the BCM50 Release 1 and have now been introduced to the BCM200 and BCM400 with the BCM 4.0 release.

BCM administrator and network manager account access management is being made more secure by enhancing passwords, account management, increasing interface security and adding audit logging. These improvements bring the BCM200 and BCM400 in alignment with the security enhancements introduced with BCM50.

Following is the list of security enhancements newly supported with BCM 4.0: These enhancements were introduced with the BCM50 platform and are now being brought to BCM200 and BCM400. Additionally, the items with two asterisks (**) are incremental to the BCM50 Release 1 security feature set.

Password Enhancements

- Password characteristics more stringent (length, criteria).
- Password aging, history, change notification.**
- Forced password change on initial login.**
- Secure Hashing Algorithm 1 (SHA1) storage of Passwords.
- Tel-set based admin requires user id and password.

Account Enhancements

- Idle timeout, disabling un-used accounts, logged in userid / access display.
- Upon account login, display of last successful login, last failed login attempt and total failed login attempts.

Increasing interface security

- Support for Secure Copy (SFTP) providing for SSH encrypted file transfers
- SNMP v2 & v3 with encryption .
- Use of digital signatures and enhanced tamper detection to ensure trusted sources for software upgrades (patches, software release upgrades).

Addition of Audit Logging

- All configuration changes entered through Element Manager are tracked by logs identifying user, time, date, data changed and modified fields.
- Security audit log tracking.

Centralized Authentication

- Radius Client support to authorize, authenticate, and manage account privileges using a centralized Radius server. Providing a single place for management of this information can result in operational cost savings. **

BCM 4.0 Security Benefits Summary

By upgrading to BCM 4.0, customers will able to:

- Enforce more secure account access controls to the BCM, to ensure secure management of the BCM and thereby increasing protection against potential vulnerabilities.

- Support IP Sec tunnels for management, including the added ability for encrypted SNMP and file transfers providing BCM users with an expanded capability set for secure interface communications.
- Monitor audit logging of login attempts providing the BCM user the ability to track security violation attempts and determine if further action is required.
- Minimize impacts of potential vulnerabilities, attacks and tampering
- Reduce Administrative & Support overhead through the use of Radius server for centralized account administration.
- Increase overall Security with effective logging capabilities for Audit Trail logs, Alarm logs, Configuration Change logs, including traceability of configuration changes to user ids and interfaces.

SRG200/400 RIs1.5 Benefits

By upgrading to SRG 1.5, customers will able to:

- Migrate the SRG 1.0 installed base systems to leverage Linux operating system.
- Take advantage of new security and management paradigm of the BCM platform .

Order your BCM 4.0 or SRG200/400 RIs1.5 Upgrade Now!

The BCM 4.0 and SRG200/400 RIs1.5 upgrades are now available for ordering. Please refer to the Global Product and Pricing Catalogue for availability dates in your region and remember to check the Partner Information Center to find out about applicable Marketing Rebate Promotions.

REQUIRED ACTIONS

See RECOMMENDATIONS

ATTACHMENTS

There are no attachments for this bulletin

NORTH AMERICA

1 800 4-NORTEL
(1 800 466-7835)

EUROPE, MIDDLE EAST & AFRICA

00800 8008 9009
+44 (0)870-907-9009

ASIA PACIFIC

+61 2-8870-8800

<http://www.nortel.com>