

Product Advisory Alert

Bulletin Number: PAA-2004-0187-Global-Rev.2

Date: 4 June 2004

Note this bulletin is replacing previously released bulletin – PAA-2004-0187-Global-Revision 1.0, issued on 7 May 2004

BCM Security Advisory: BCM Patch Update for MS04-011

Problem Description

This is an updated bulletin, announcing the availability of the Business Communications Manager (BCM) Patch Update for the Security Update for Microsoft Windows (835732) for vulnerabilities described in the Microsoft Security Bulletin MS04-011, announced by Microsoft on 13 April 2004.

According to Microsoft, some of these vulnerabilities on applicable environments could potentially allow an attacker to execute arbitrary code on a system, lead to privilege escalation, cause a denial of service attack, or lead to other system compromises.

The BCM 3.6 and BCM 3.5 Patch Updates for the Security Update for Microsoft Windows related to MS04-011 are being released to resolve these potential issues. After the BCM Patch Update has been applied, the BCM will no longer be susceptible to the referenced Microsoft security advisory bulletin MS04-011 security vulnerabilities identified by Microsoft.

Please refer to the Nortel Networks bulletin PAA-2004-0187-Global Rev 1.0 issued on 7th May 2004, posted on the Partner Information Center (PIC), for an outline of Microsoft security advisory bulletins MS04-011, MS04-012, MS04-013 and MS04-014 vulnerabilities as they pertain to BCM.

Expected Scope

Business Communications Manager (BCM) software releases BCM 3.6, BCM 3.5, BCM 3.0.1, BCM 3.0 and BCM 2.5 FP1 MR are affected, applicable to all BCM hardware platforms. Software releases prior to BCM 2.5 FP1 MR (BCM 2.5 FP1, BCM 2.5, BCM 2.0x) which have been “Manufacture Discontinued” are also affected, but have not been tested or analyzed, and are not supported.

Expected Solution

The BCM 3.6 and BCM 3.5 Patch Updates for the Security Update for Microsoft Windows related to MS04-011 are being released to resolve the potential vulnerabilities identified by Microsoft.

Note that the Microsoft Patch “Hotfix” should not be applied directly to the BCM system, unless directed by Nortel Networks.

The BCM 3.5 Patch Update can be installed on systems with BCM 3.5 software load, while the BCM 3.6 Patch Update can be installed on systems with BCM 3.6 software load. The Patch Updates are applicable to all BCM hardware platforms.

The BCM 3.5 Patch Update is projected to be Generally Available by 4th June 2004 and the BCM 3.6 Patch Update is projected to be Generally Available by 11th June 2004. The approximately 3.39 megabyte Patch Update is delivered to the BCM by means of the BCM Update Wizard. The Patch Update can either be applied immediately on the targeted system or downloaded and applied at a later time. It will automatically initiate a system restart in order to take effect. After the Patch Update has been applied, the BCM will no longer be susceptible to the referenced Microsoft security advisory bulletin MS04-0011 for the security vulnerabilities identified by Microsoft.

The BCM 3.6 and BCM 3.5 Patch Updates will be made available through Nortel Networks' normal BCM Patch Update distribution process.

BCM Patch Updates are posted and available to distributors and partners from the secure Partner Information Center (PIC) site URL at <http://www.nortelnetworks.com/pic> (Partner Information Center / Support / Business Communications Manager / Software). Partners may also register for notification of new Patch Updates posted on PIC (Partner Information Center / Support / Register).

For customers with larger BCM networks, Nortel Networks recommends the use of the Network Configuration Manager, NCM, to automate the process of distributing and applying Patch Updates to a network of BCM systems over an IP network. With NCM 3.6, Patch Update distribution and application can be scheduled for BCM 3.6, 3.5, 3.0.1 and 3.0 systems, thereby dramatically reducing the time required to deploy the Patch Updates to many BCM systems. For more information about NCM, please consult the NCM Application Brief available on the Partner Information Center, PIC.

Note that some concerns had been raised regarding some of the vulnerabilities identified in the cumulative Microsoft Security Update for Microsoft Windows (MS04-011). The BCM is **not** impacted by these vulnerabilities identified below:

- (a) LSASS Vulnerability (CAN-2003-0533)
- (b) PCT Vulnerability (CAN-2003-0719)

Please refer to Nortel Networks for bulletin PAA-2004-0187-Global Rev 1.0, issued on 7th May 2004 posted on PIC, and to <http://www.microsoft.com/technet/security/Bulletin/MS04-011.mspx> for details on the Microsoft MS04-011 for details.

Recommended Action

It is recommended that the BCM Patch Updates related to the Security Update for Microsoft Windows Microsoft MS04-011 vulnerabilities be applied to BCM systems with BCM 3.5 and BCM 3.6 software releases.

Nortel Networks is not aware of any exploitation of BCM of the announced Microsoft MS04-011 Security Update for Microsoft Windows vulnerabilities. As usual, Nortel Networks recommends customers create a company-wide security and virus protection policy for all elements of their network to reduce the threat of malicious attacks. While the application of such a policy will continue to reduce the threat of future malicious attacks, the application of the Patch Update described herein

removes the threat to the BCM of any exploitation specific to the referenced Microsoft security advisory bulletin MS04-011 for the security vulnerabilities identified by Microsoft.

Nortel Networks suggests safeguarding your network to minimize the potential of future malicious exploitations, and recommends using the BCM's built-in firewall rules for limiting access to known trusted endpoints to protect the BCM.

Nortel Networks recommends that any PC Clients connecting to the BCM have the Microsoft security hotfixes issued by Microsoft security bulletins installed as recommended by Microsoft.

Customers concerned about security should always consider upgrading to the latest release of BCM software to ensure they are taking advantage of the latest security measures incorporated into the product.

Customers with BCM containing earlier versions of software releases may want to consider being upgraded, using standard BCM upgrade kits that are available through normal ordering process, in order to be ready to accept Patch Updates.

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

Should there be further change in this Product Advisory Alert, the bulletin will be revised and communicated.

Fix Completion Date

The BCM 3.5 Patch Update is projected to be Generally Available by 4th June 2004 and the BCM 3.6 Patch Update is projected to be Generally Available by 11th June 2004.

References and Related Documents

Revision 1.0 and 2.0 of this BCM Product Advisory Alert PAA-2004-0187-Global bulletin for Microsoft MS04-011 through MS04-014 is available for download from Nortel Networks' Partner Information Center (PIC) website at <http://www.nortelnetworks.com/pic>.

The Microsoft Security Bulletins are available on their website, and can be viewed on-line at: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp>

For more information regarding this bulletin, please contact:

North America: 1-800-4NORTEL or 1-800-466-7835
Europe, Middle East and Africa: 00800 8008 9009, or +44 (0) 870 907 9009

Contacts for other regions are available at: <http://www.nortelnetworks.com/help/contact/global/>

Or visit the eService portal at <http://www.nortelnetworks.com/cs> under Advanced Search.

If you are a channel partner, more information can be found under <http://www.nortelnetworks.com/pic> under Advanced Search.

* Nortel Networks, the Nortel Networks logo, and the Globemark are trademarks of Nortel Networks.

Nortel Networks is an industry leader and innovator focused on transforming how the world communicates and exchanges information. The Company is supplying its service provider and enterprise customers with communications technology and infrastructure to enable value-added IP data, voice and multimedia services spanning Wireless Networks, Wireline Networks, Enterprise Networks, and Optical Networks. As a global Company, Nortel Networks does business in more than 150 countries. More information about Nortel Networks can be found on the Web at www.nortelnetworks.com.