Product Advisory Alert

Bulletin Number: PAA-2004-0045-Global
Issue: 1.0
Date: 13 February 2004

BCM Product Security Advisory – Impacts of Microsoft Security Bulletins MS04-005 through MS04-007

Problem Description

This Advisory Alert outlines Nortel Networks Business Communications Manager (BCM) position on susceptibility to attacks that exploit the recently identified vulnerabilities described in Microsoft security advisory bulletins MS04-005, MS04-006 and MS04-007 announced by Microsoft on Tuesday, February 10th, 2004. According to Microsoft, some of these vulnerabilities on applicable environments could potentially allow an attacker to run arbitrary code on a system, or lead to privilege escalation, which could result in a buffer overrun, or other system compromise.

The Business Communications Manager (BCM) runs on Microsoft Windows based operating systems for its applications and IP Telephony. This bulletin is related to the above Microsoft security advisory bulletins and identifies any potential impacts to affected BCM releases, available BCM patches or workarounds and recommended actions.

Scope

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

Expected Solution

Nortel Networks has performed analysis and / or testing on the BCM systems with the following results.

Note that the Microsoft Patch “Hotfix” information has been provided for reference only. Any of the Microsoft Patch “Hotfix” should not be applied directly to the BCM system, unless directed by Nortel Networks.

Microsoft Published	Microsoft Bulletin	Microsoft Patch "Hotfix"	Microsoft Rating	Microsoft Description	BCM System Result
Feb 10, 2004	**MS04-005**	835150	Important	Vulnerability in Virtual PC for Mac could lead to privilege elevation.	No BCM Impact
Feb 10, 2004	**MS04-006**	830352	Important (Low for Win NT4.0 Embedded)	Vulnerability in the Windows Internet Naming Service (WINS) Could Allow Code Execution.	**Rated Low Impact on BCM**
Feb 10, 2004	**MS04-007**	828028	Critical	ASN.1 Vulnerability Could Allow Code Execution.	**BCM Impacted**

Nortel Networks is in the final stages of testing the patch that fixes this issue referenced in Microsoft security advisory bulletin MS04-007 for the ASN.1 vulnerability identified by Microsoft. The BCM patch for BCM 3.5 is intended to be Generally Available on Friday Feb 13th, 2004, and the patch for BCM 3.0, 3.0.1 and 2.5 FP1 MR. intended to be Generally Available by Friday Feb 18th, 2004. The patches will be applicable to all BCM hardware platforms.

The patch will be made available through Nortel Networks' normal BCM patch distribution process. The patch 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. The patch can be applied to individual BCMs or can be applied to a network of BCMs using the BCMs Network Configuration Manager (NCM). After the patch has been applied, the BCM will no longer be susceptible to the referenced Microsoft security advisory bulletin MS04-007 for the ASN.1 vulnerability identified by Microsoft.

Recommended Action

It is recommended that the BCM patch related to the Microsoft MS04-007 ASN.1 vulnerability be applied to BCM 3.5, 3.0.1, 3.0 and 2.5 FP1 MR systems.

Nortel Networks is not aware of any exploitation of the recently announced Microsoft MS04-007 ASN.1 vulnerability. As usual, Nortel Networks recommends customers create a company-wide security and virus protection policy for all elements of their network. While the application of such a policy will continue to reduce the threat of future malicious attacks, the application of the patch described herein removes the threat to the BCM of any exploitation specific to the referenced Microsoft security advisory bulletin MS04-007 for the ASN.1 vulnerability identified by Microsoft.

Nortel Networks recommends that any PC Clients connecting to the BCM have the security hotfixes for the following Microsoft security alert bulletins installed as recommended by Microsoft: MS04-005, MS04-006 and MS04-007.

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 pre-2.5 FP1 MR software 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 the patches.

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

References and Related Documents

This BCM product advisory bulletin for Microsoft MS04-007 ANS.1 vulnerability is available for download from Nortel Networks' Partner Information Center (PIC) website at www.nortelnetworks.com.

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 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.