Product Advisory Alert

Bulletin Number: PAA 2003-0290-Global
Issue: 3.0
Date: 24 September 2003

BCM Product Security Advisory – Patch for Microsoft RPC Vulnerabilities (MS03-039 and MS03-026)

Nortel Networks would like to announce the availability of a patch for Nortel Networks Business Communications Manager (BCM) to address both of the recently announced Microsoft RPC vulnerabilities (CERT Advisories CA-2003-23 and CA-2003-16). Customers concerned about security should consider downloading and applying this patch. **Application of this patch addresses both Microsoft Vulnerability MS03-039 and MS03-026.** Customers who have previously deployed the BCM patch released specifically for MS03-026 will need to apply this newest patch to fully address the two vulnerabilities. Note that the previous patch, which only addresses the MS03-026 vulnerability, **must not** be applied after the current patch. Doing so will overwrite the files that are required to remove the MS03-039 vulnerability.

As identified in previous issues of this Nortel Networks Product Advisory Alert (PAA 2003-0290-Global Issues 1 and 2), the current BCM embedded operating system may be impacted by the referenced Microsoft vulnerabilities.

The less than two megabyte patch is now available through Nortel Networks' normal BCM patch distribution process, and can be installed on BCM 2.5 FP1, BCM 2.5 FP1 MR1, BCM 3.0, and BCM 3.0.1 software loads, and will be applicable to all BCM hardware platforms. (See below for instructions on where to find the patch for downloading.). The patch is delivered to the BCM via a wizard. It can either be applied immediately on the targeted system or downloaded and applied later. The patch will automatically initiate a system restart in order to take effect. After the patch has been applied, the BCM will no longer be susceptible to future attacks that attempt to exploit either of the Microsoft RPC vulnerabilities (MS03-039 or MS03-026). Several vendors have released updates to tools that help network administrators to identify devices that are vulnerable to exploitations of these vulnerabilities. We have identified issues with Microsoft's current version (KB824146) in falsely identifying unpatched BCM systems as not vulnerable and are working to resolve this discrepancy with Microsoft. While we do not endorse the use of any specific vendor's products, in our internal testing of some other scanners such as the *Retina RPC DCOM Scanner v 1.1.0* (eEye Digital Security), both unpatched and patched BCM systems were correctly identified.

The **BCM has not, to Nortel Networks knowledge, as of this date been compromised** by any exploitations of the RPC vulnerabilities identified in MS03-039 and MS03-026. In Product Advisory Alert PAA 2003-0290-Global Issue 1, Nortel Networks identified how to use the BCM firewall to minimize the risk of exposure of the BCM to undesirable security threats that attempt to exploit the RPC vulnerability. Nortel Networks also recommends customers create a company-wide security and virus protection policy for all elements of their network. While the use of such a policy will continue to reduce the threat of future malicious attacks, the application of the patch described herein addresses the threat to the BCM of any future exploitations of the *specific* Microsoft RPC vulnerability identified in CERT Advisory CA-2003-23 and CA-2003-16.

These vulnerabilities will also be addressed in our upcoming BCM 3.5 software release, which is currently scheduled for General Availability (GA) in October 2003.

To download the patch:

Access the Nortel Networks web site and follow the Software Download link in the Support section. Select the Business Series product family and then select the Business Communications Manager Software link. The following two patches will be listed:

- BCM 3.0/3.0.1 – RPC Patch (MS03-039/026)
- BCM 2.5 FP1/MR1 – RPC Patch (MS03-039/026)

BCM patches are only available to authorized distributors, so you will be prompted to enter a valid User ID and Password before downloading the patch.

For more information go to:

Nortel Networks Product Advisory Alert PAA 2003-0290-Global Issue 1
https://app12.nortelnetworks.com/cgi-bin/mynn/home/NN_bulletinDetails.jsp?DC=54&DY=2003&curOid=12460&whereClause=10&progSrcID=-8461

Nortel Networks Response to CERT Advisory CA-2003-16
http://www142.nortelnetworks.com/bvdoc/cs/supportnews/v6_Nortel_CERT_Advisory_CA-2003-16.pdf

CERT Advisory CA-2003-23
<http://www.cert.org/advisories/CA-2003-23.html>

CERT Advisory CA-2003-16
<http://www.cert.org/advisories/CA-2003-16.html>

Microsoft Security Bulletin MS03-039
http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-039.asp

Microsoft Security Bulletin MS03-026
http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp