TECHNICAL BULLETIN

SECURITY ADVISORY

LEGACY REF ID

STATUS **WORKING**

PRIORITY **MAJOR**

ACTIVE/RETIRED DATE

FAMILY	LINE	PRODUCT
BCM BCM	BCM BCM	BCM Survivable Remote Gateway

SOFTWARE AFFECTED RELEASE	BCM 3.6, BCM 3.5, SRG 1.0
SW FIXED REL	BCM 3.7
PREREQUIRED PATCH	
PATCH ID	
REFERENCE ID	Security Advisory 2005005705
REGION	All
REPLACES	
REPLACED BY	
FUNCTION	Security Advisory
AUTHOR	ABDULLA, NASHIR (NABDULLA)

BCM AND SRG SECURITY ADVISORY PATCH UPDATE FOR MS05-019

BACKGROUND

This Security Advisory bulletin announces the availability of Nortel Patch Updates for the Business Communications Manager (BCM) and the Survivable Remote Gateway (SRG) that addresses issues for the vulnerabilities described in the Microsoft Security Bulletin MS05-019, announced by Microsoft on 12 April 2005.

ANALYSIS

PROBLEM DESCRIPTION:

This Security Advisory bulletin identifies any potential impacts to affected BCM and / or SRG releases, available patch updates or workarounds and / or recommended actions, related to the Microsoft Knowledge Based Article 893006 for vulnerabilities described in the Microsoft Security Bulletin MS05-019, announced by Microsoft on 12 April 2005. The Business Communications Manager (BCM) and the Survivable Remote Gateway (SRG) system runs on Microsoft Windows based operating systems for its applications and IP Telephony.

According to Microsoft, some of the vulnerabilities for MS05-019 on applicable environments could potentially allow remote code execution on a system or cause a denial of service.

The BCM 3.6, BCM 3.5 and SRG 1.0 Patch Updates are being released to address the vulnerabilities described by Microsoft in MS05-019. After the Patch Updates have been applied,

the BCM and / or SRG system will no longer be susceptible to the security vulnerabilities identified by Microsoft.

Note that on 11 May 2005, Microsoft updated bulletin MS05-019 to advise customers that they plan to re-release the MS05-019 security update in June, 2005. As a result, it may be necessary to re-release the Nortel BCM and SRG Patch Updates, at which time this Security Advisory Bulletin will be revised if necessary. Prior to the possible re-release of any BCM and SRG security Patch Updates related to MS05-019 is available, BCM or SRG customers experiencing the symptoms described in the Microsoft Knowledge Base Article 898060 (http://support.microsoft.com/kb/898060/) should contact Nortel Technical Support.

EXPECTED SCOPE:

The following Business Communications Manager (BCM) and the Survivable Remote Gateway (SRG) products are affected and covered in this bulletin: BCM 3.5, BCM 3.6 and SRG 1.0, applicable to all BCM 200, BCM 400 and BCM 1000 platforms.

Releases prior to BCM 3.5 which have been Manufacture Discontinued, and no longer supported under BCM lifecycle support guidelines, are also affected, but have not been tested or analyzed, as they are not supported.

EXPECTED SOLUTION:

Note that the Microsoft Update should NOT be applied directly to the BCM / SRG system, unless directed by Nortel Networks.

The Nortel Patch Updates for BCM 3.6, BCM 3.5 and SRG 1.0 are being released to resolve the potential vulnerabilities identified by Microsoft in MS05-019.

Issues identified by Microsoft in bulletin MS05-019 have been addressed in BCM 3.7, which will therefore not be impacted.

The BCM 3.5 Patch Update can be applied to systems with BCM 3.5 software load, while the BCM 3.6 Patch Update can be applied to systems with BCM 3.6 software load and the SRG 1.0. The Patch Updates are applicable to all BCM 200, BCM 400 and BCM 1000 platforms.

The Nortel Patch Updates for BCM 3.5, BCM 3.6 and SRG 1.0 are projected to be Generally Available by 20 May 2005. The approximately 1.02 megabyte Patch Update is delivered 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 or SRG will no longer be susceptible to the security vulnerabilities identified by Microsoft in the Microsoft Security Bulletin MS05-019.

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

BCM and SRG 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 / Technical Support / Business Communications Manager / Software, Partner Information Center / Technical Support / Succession / Survivable Remote Gateway / 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 and 3.5 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.

RECOMMENDATIONS

RECOMENDED ACTION:

It is recommended that the Nortel BCM / SRG Patch Updates, for Microsoft Windows related to vulnerabilities described in MS05-019, be applied to BCM 3.5, BCM 3.6 and SRG 1.0 systems.

Note that the Microsoft Update should NOT be applied directly to the BCM / SRG system, unless directed by Nortel Networks.

Nortel Networks is not aware of any exploitation of the BCM or SRG for Microsoft Windows vulnerabilities announced in the Microsoft Security Bulletin MS05-019. 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 and SRG of the exploitation specified in the referenced Microsoft Security Bulletin MS05-019 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 built-in firewall rules for limiting access to known trusted endpoints to protect the BCM and SRG.

Nortel Networks recommends that any PC Clients connecting to the BCM or SRG have the Microsoft security updates 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 Security Advisory, the bulletin will be revised and communicated.

REQUIRED ACTIONS

It is recommended that the Nortel Patch Updates related to the Security Update for Microsoft Windows MS05-019 vulnerabilities be applied to BCM 3.5, BCM 3.6 and SRG 1.0 systems.

Note that the Microsoft Update should NOT be applied directly to the BCM / SRG system, unless directed by Nortel Networks.

ATTACHMENTS

There are no attachments for this bulletin

FOOTER INFORMATION

FOR ADDITIONAL INFORMATION

FIX COMPLETION DATE:

The Nortel Patch Updates related to MS05-019 are projected to be posted for BCM 3.6, BCM 3.5 and SRG 1.0 by 20 May 2005.

Issues identified by Microsoft in bulletin MS05-019 have been addressed in BCM 3.7, which will therefore not be impacted.

REFERENCES AND RELATED DOCUMENTS:

This Security Advisory Bulletin for Microsoft MS05-019 is available for download from Nortel Networks' Partner Information Center (PIC) website at http://www.nortelnetworks.com/pic and the Nortel Networks Technical Support website at http://nortel.com/securityadvisories

Please refer to http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx for details on MS05-019 that also covers the following Microsoft Knowledge Based Articles: 893066, 890345, 896350, 897656 and 898060. The Microsoft Security Bulletins are available on their website, and can be viewed on-line at: http://www.microsoft.com/technet/security/current.aspx

Nortel's recommendation for any maintenance type activities listed in this bulletin should be completed during the local maintenance window.

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
Asia Pacific: +61 2-8870-8800

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 is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at http://www.nortel.com.

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