

2005006045
DOCUMENT ID

1
VERSION

LEGACY REF ID

STATUS **ACTIVE**

PRIORITY **MAJOR**

ACTIVE DATE **2005-07-05**

TECHNICAL BULLETIN

SECURITY ADVISORY

FAMILY BCM BCM	LINE BCM BCM	PRODUCT BCM Survivable Remote Gateway
SOFTWARE AFFECTED RELEASE	BCM 3.7, BCM 3.6, BCM 3.5, SRG 1.0	
SW FIXED REL		
PREREQUIRED PATCH		
PATCH ID		
REFERENCE ID	Security Advisory 2005006010.v2	
REGION	All	
REPLACES		
REPLACED BY		
FUNCTION	Security Advisory	
AUTHOR	ABDULLA, NASHIR (NABDULLA)	

BCM AND SRG SECURITY ADVISORY PATCH UPDATE FOR MS05-027

BACKGROUND

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 896422 for vulnerabilities described in the Microsoft Security Bulletin MS05-027, announced by Microsoft on 14 June 2005.

This Security Advisory bulletin is applicable to the Business Communications Manager (BCM) and the Survivable Remote Gateway (SRG) systems running on Microsoft Windows based operating systems for its applications and IP Telephony.

According to Microsoft, some of the vulnerabilities for MS05-027 on applicable environments could potentially allow remote code execution on a system.

ANALYSIS

The following Business Communications Manager (BCM) and the Survivable Remote Gateway (SRG) products are affected and covered in this bulletin: BCM 3.7, BCM 3.6, BCM 3.5 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.

The BCM50 is NOT impacted.

The Nortel Patch Updates for BCM 3.7, BCM 3.6, BCM 3.5 and SRG 1.0 are being released to address the potential vulnerabilities identified by Microsoft in MS05-027, and are projected to be Generally Available by 5 July 2005. 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: The Nortel Patch Updates that must be applied to the SRG 1.0 system must match the software release that the SRG is based on. The Nortel Patch Update for a BCM 3.6-based SRG 1.0 system is different from the Nortel Patch Update for a BCM 3.7-based SRG 1.0 system.

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

RECOMMENDATIONS

It is recommended that the Nortel BCM / SRG Patch Updates, for Microsoft Windows related to vulnerabilities described in MS05-027, be applied to BCM 3.7, BCM 3.6, BCM 3.5 and SRG 1.0 systems.

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

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

Nortel is not aware of any exploitation of the BCM or SRG for Microsoft Windows vulnerabilities announced in the Microsoft Security Bulletin MS05-027. As usual, Nortel 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 MS05-027 for the security vulnerabilities identified by Microsoft.

Nortel 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 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 or SRG systems 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 BCM / SRG Patch Updates related to the Security Update for Microsoft Windows MS05-027 vulnerabilities be applied to BCM 3.7, BCM 3.6, BCM 3.5 and SRG 1.0 systems.

NOTE: The Nortel Patch Updates that must be applied to the SRG 1.0 system must match the software release that the SRG is based on. The Nortel Patch Update for a BCM 3.6-based SRG 1.0 system is different from the Nortel Patch Update for a BCM 3.7-based SRG 1.0 system.

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

The approximately 1.11 megabyte Nortel 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 MS05-027.

The BCM and SRG Patch Updates will be made available through Nortel's 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 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 3.7, BCM 3.6 and BCM 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.

ATTACHMENTS

There are no attachments for this bulletin

FOOTER INFORMATION

FOR ADDITIONAL INFORMATION

This Security Advisory Bulletin for Microsoft MS05-027 is available for download from Nortel's Partner Information Center (PIC) website at <http://www.nortelnetworks.com/pic> and the Nortel Technical Support website at <http://nortel.com/securityadvisories>

Please refer to the Microsoft website <http://www.microsoft.com/technet/security/Bulletin/MS05-027.msp> and the related Microsoft Knowledge Based Article 896422 for details on vulnerabilities described in the Microsoft Security Bulletin MS05-027. 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, the Nortel logo and the Globemark are trademarks of Nortel.

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>