



## Nortel Enterprise Response to Sockstress TCP DoS (Outpost24 TCP Issues)

### Source:

CERT-FI Advisory on the Outpost24 TCP Issues at:  
<https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>  
CVE-2008-4609 at:  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4609>  
Microsoft Bulletin MS09-048 is available at:  
<http://www.microsoft.com/technet/security/Bulletin/MS09-048.msp>

**BULLETIN ID:** 2009009801, Rev 1  
**PUBLISHED:** 2009-10-15  
**STATUS:** Active  
**REGION:** All  
**PRIORITY:** Critical  
**TYPE:** Security Advisory

### Overview:

The vulnerabilities described in this advisory can potentially affect systems and applications that run an implementation of TCP protocol (RFC793 et al.). The issues were found by the Sockstress tool developed by Outpost24 and reported by CERT-FI.

Sockstress is an user-land TCP socket stress testing framework that can open an arbitrary number of sockets. The attacks use different variations in terms of payloads, window sizes and stalling TCP states. The attacks take advantage of the exposed resources the target makes available post TCP handshake, namely kernel and system resource such as counters, timers, and memory pools. The attacks do not require significant bandwidth.

General impact of the tool and attack scenarios is a denial of service (DoS). However, the impact varies by stack implementation. The overall impact on a given setup depends on the target application and the operating system running on the target. The impact on specific systems falls into three categories:

#### 1) Temporary impact on the application

CVSS Vector and score: AV:N/AC:M/Au:N/C:N/I:N/A:P - 4.3

The application fails to accept connections from legitimate users when the attack is ongoing. This state is temporary and the application will become usable once the attack stops.

#### 2) Permanent impact on the application

CVSS Vector and score: AV:N/AC:M/Au:N/C:N/I:N/A:P - 4.3

The application fails to accept connections from legitimate users once the attack has started and lasted for some period of time. This state is permanent in the sense that the application will not become responsive until it has been restarted.

#### 3) Permanent impact on the system

CVSS Vector and score: AV:N/AC:M/Au:N/C:N/I:N/A:C - 7.1

The system (the OS kernel) stops performing its essential functions once the attack has been started and has lasted for some period of time. As a result, the system will be unusable. The system becomes usable once it has been rebooted.

The severity of the attacks range from a CVSS score of 4.3 (medium severity) through 7.1 (high severity) depending on the persistence and scope of the DoS condition.

Before taking any action please ensure that you are viewing the latest official version of this security advisory by referencing <http://www.nortel.com/securityadvisories>

For more information:

Please contact your next level of support or visit <http://www.nortel.com/contact> for support numbers within your region.

Nortel security advisories: <http://nortel.com/securityadvisories>

Nortel Partner Information Center (PIC) website: <http://www.nortelnetworks.com/pic>

## Symptoms:

Please refer to the Resolution section herein for product-specific information from Nortel.

## Prevention:

Please refer to the Resolution section herein for product-specific information from Nortel.

## Mitigation:

Please refer to the CERT-FI link in the Source section for mitigation information for the various vulnerabilities addressed by the CERT-FI advisory. Please refer to the Resolution section herein for product-specific information from Nortel.

## Risk:

Please refer to the CERT-FI link in the Source section for additional information about the risks of the various vulnerabilities addressed by the CERT-FI advisory. Please refer to the Resolution section of this bulletin for product-specific information from Nortel.

## Resolution:

1) The following Nortel Generally Available products are potentially vulnerable to the security issue outlined in the CERT-FI Advisory on the Outpost24 TCP Issues bulletin. Please refer to product-specific text below for instructions on how to proceed.

CallPilot - 201i, 202i, 600r, 703t, 1002rp, 1005r

. Microsoft patch MS09-048 KB967723 has been tested and approved for installation on CallPilot servers. See bulletin P-2009-0001-Global-Rev9\_CallPilot Server Security Update for details.

Contact Center - CCT

. Microsoft Windows based components are addressed by MS09-048 - Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723) Nortel Security Bulletin Number: 2009009717, Rev 1.

Contact Center - Multimedia Agent Desktop Display, CCMM, Outbound

. Contact Center portfolio product servers depend on TCP/IP implementation by Windows. Microsoft provides MS09-048 security hotfix to address the TCP DoS vulnerability. It is Nortel recommendation to apply MS09-048 security hotfix to all applicable Contact Center portfolio product servers.

Contact Center - Manager CCMA, CCMS, Express, NCC

. Contact Center portfolio product servers depend on TCP/IP implementation by Windows. Microsoft provides MS09-048 security hotfix to address the TCP DoS vulnerability. It is Nortel recommendation to apply MS09-048 security hotfix to all applicable Contact Center portfolio product servers

Contact Center - Agent Greeting

. Contact Center portfolio product servers depend on TCP/IP implementation by Windows. Microsoft provides MS09-048 security hotfix to address the TCP DoS vulnerability. It is Nortel recommendation to apply MS09-048 security hotfix to all applicable Contact Center portfolio product servers.

#### Call Center - Symposium Agent, TAPI Server

. Contact Center portfolio product servers depend on TCP/IP implementation by Windows. Microsoft provides MS09-048 security hotfix to address the TCP DoS vulnerability. It is Nortel recommendation to apply MS09-048 security hotfix to all applicable Contact Center portfolio product servers

#### Ethernet Routing Switch 2500 - 2526T, 2526T-PWR, 2550T, 2550T-PWR

. During attack, previously established/existing traffic is not disrupted (no change). During attack, new TCP connections are prevented while attack is in progress. The devices do not crash. Devices recover gracefully after the attack.

#### Ethernet Routing Switch 4500 - 4524GT, 4526FX, 4526G-PWR, 4526GTX, 4526T, 4526T-PWR, 4550T, 4524GT-PWR, 4548GT-PWR, 4550T-PWR

. During attack, previously established/existing traffic is not disrupted (no change). During attack, new TCP connections are prevented while attack is in progress. The devices do not crash. Devices recover gracefully after the attack.

#### Ethernet Routing Switch 5000 - 5650TD, 5698TFD, 5650TD-PWR, 5698TFD-PWR

. During attack, previously established/existing traffic is not disrupted (no change). During attack, new TCP connections are prevented while attack is in progress. The devices do not crash. Devices recover gracefully after the attack.

#### Ethernet Routing Switch - 8600

. TCP Socket stress testing against the ERS 8600 has shown a negative impact on CPU utilization as well as temporary loss of remote access to the switch. While the data path is not directly impacted, the additional load on CPU utilization may affect layer 3 functionality and disrupt normal function of the ERS 8600 within the network. Removal of the Sockstress DoS attack stimulus allows the switch to recover. Impact to the switch may be mitigated or avoided completely through the use of Access Policies configured to limit access to TCP based services from trusted hosts or subnets only.

#### Multimedia Communications - MAS

. Microsoft Windows based components are addressed by MS09-048 - Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723) Nortel Security Bulletin Number: 2009009717, Rev 1.

For Solaris based components, a final resolution is pending completion from Sun Microsystems. Nortel is currently awaiting this patch so that we may test. Updates will be made available as this situation progresses.

#### Secure Network Access - Identity Engines Ignition Server

. NIEIS Ignition Server is vulnerable to Sockstress TCP as it uses Red Hat Linux 5.3. Red Hat do not plan to release updates to resolve these issues; however, the effects of these attacks can be reduced with the following mitigation procedure found on <http://kbase.redhat.com/faq/docs/DOC-18730>

#### Secure Network Access - Identity Engine Ignition Analytics, Identity Engine Guest Manager, Identity Engine Ignition Posture

. Microsoft Windows based components are addressed by MS09-048 - Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723), it is recommended that customers install the Microsoft patch according to Microsoft directions.

#### Secure Network Access - Switch 4050, Switch 4070

. Red Hat do not plan to release updates to resolve these issues; however, the effects of these attacks can be reduced with a mitigation procedure found on <http://kbase.redhat.com/faq/docs/DOC-18730>

#### Self-Service - Media Processing Svr 100, 500, 1000

. Microsoft Windows based components are addressed by MS09-048 - Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723) Nortel Security Bulletin Number: 2009009717, Rev 1.

For Solaris based components, a final resolution is pending completion from Sun Microsystems. Nortel is currently awaiting this patch so that we may test. Updates will be made available as this situation progresses.

#### Self-Service - Peri Application, Peri Workstation, Peri CTI, Peri IVR, Peri NT Server, Speech Server

. Microsoft Windows based components are addressed by MS09-048 - Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723) Nortel Security Bulletin Number: 2009009717, Rev 1.

For Solaris based components, a final resolution is pending completion from Sun Microsystems. Nortel is currently

awaiting this patch so that we may test. Updates will be made available as this situation progresses.

#### Self-Service - CCSS7, CCXML, VoiceXML, WVADS

. Microsoft Windows based components are addressed by MS09-048 - Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723) Nortel Security Bulletin Number: 2009009717, Rev 1.

For Solaris based components, a final resolution is pending completion from Sun Microsystems. Nortel is currently awaiting this patch so that we may test. Updates will be made available as this situation progresses.

#### Self Service - Video Server, CDD

. Microsoft Windows based components are addressed by MS09-048 - Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723) Nortel Security Bulletin Number: 2009009717, Rev 1.

For Solaris based components, a final resolution is pending completion from Sun Microsystems. Nortel is currently awaiting this patch so that we may test. Updates will be made available as this situation progresses.

#### Switched Firewall - SF-5109, SF-5114, SF/VPN 5124, SFA-6400, SFA-6600

. Check Point released a hotfix for VPN-1 Power/UTM and VPN-1 Pro/Express: R65 HFA\_50, R62 HFA\_01, R60 HF\_A07 and are available for download from the Check Point support center. Customers are required to first upgrade to the latest HFA on top of which the hotfix is available and then install the required hotfix. Download the hotfix associated with Linux platform and follow the Check Point release notes for the installation procedure.

2) The following Nortel Generally Available products are not vulnerable to the security issue outlined in the CERT-FI Advisory on the Outpost24 TCP Issues. Please refer to product-specific information below for any further instructions.

#### BCM - BCM50, BCM200, BCM400, BCM450, BCM1000, SRG200, SRG400

. The Linux BCM (and BCM-based SRG) products perform as expected and are not adversely impacted when subjected to the potential Sockstress TCP DoS

. The BCM / SRG Win NT4 based products are no longer supported and have not been tested to understand if there are any impacts to the products from the Sockstress TCP DoS (Outpost24 TCP Issues) potential vulnerabilities. Customers concerned about security, and customers with BCM or SRG systems containing earlier versions of software releases (including BCM Release 3.x or SRG Release 1.0 (based on BCM Release 3.x)), should always consider upgrading to the latest release of BCM / SRG software, using standard BCM upgrade kits that are available through normal ordering process, to ensure they are taking advantage of the latest security measures incorporated into the product and in order to be ready to accept Patch Updates. Nortel strongly recommends upgrading to the latest release of BCM / SRG software to reduce potential security exposures.

#### Contact Center - Remote Agent Observe

. Contact Center Remote Agent Observe is not a Windows based product and the TCP/IP function is not an integral portion of the product itself.

#### Enterprise NMS - ENMS

. Since in most cases ENMS is installed in private network (intranet) where access from public network is not allowed, this vulnerability will not likely occur for ENMS. However, as a safe practice Nortel recommends user to install the patch provided by the respective vendor (i.e. Microsoft and/or Sun) as appropriate.

#### Enterprise VoIP- - TM-CS1000

. TM is not impacted by MS09-048 - Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723) - and therefore also not impacted by Sockstress TCP DoS (Outpost24 TCP Issues). However the Windows platform running Microsoft OS used for TM should have the Microsoft update MS09-048 installed as per Microsoft.

#### Ethernet Routing Switch - 3510-24T, 5510-24T, 5510-48T, 5530-24FD, 5520-24T, 5520-48T

#### Ethernet Routing Switch - 325-24G, 325-24T, 380-24T, 420-24T, 425-24T, 425-48T

#### Ethernet Routing Switch - 460-24T, 470-24T, 470-48T, BPS 2000

Messaging - NMS Mail System, Meridian Mail Compact Opt., Meridian Mail EC11, Meridian Mail MP, Meridian Mail Mod. Option, Meridian Mail Modular EC, Meridian Mail Modular GP, Meridian Mail NT/XT, Meridian Option 11 Mail

Norstar Applications - PC Console, Personal Productivity Suite

. Norstar KSUs and M7000 Series sets (including CTI, CTE & TAPI) are not impacted by the Sockstress TCP DoS (Outpost24 TCP Issues).

Norstar Core - 3X8, CICS, MICS

. Norstar KSUs and M7000 Series sets (including CTI, CTE & TAPI) are not impacted by the Sockstress TCP DoS (Outpost24 TCP Issues).

Norstar Messaging - Desktop Messaging, Flash ACD, Norstar Voice Mail

. Norstar KSUs and M7000 Series sets (including CTI, CTE & TAPI) are not impacted by the Sockstress TCP DoS (Outpost24 TCP Issues).

Norstar Peripherals - Norstar VoIP Gateway

. Norstar KSUs and M7000 Series sets (including CTI, CTE & TAPI) are not impacted by the Sockstress TCP DoS (Outpost24 TCP Issues).

Survivable Remote Gateway 1.0 - SRG200 1.0, SRG400 1.0

. The SRG 1.0 Win NT4 based product is no longer supported and has not been tested to understand if there are any impacts to the products from the Sockstress TCP DoS (Outpost24 TCP Issues) potential vulnerabilities. Customers concerned about security, and customers with SRG systems containing earlier versions of software releases (SRG Release 1.0 (based on BCM Release 3.x)), should always consider upgrading to the latest release of SRG software, using standard upgrade kits that are available through normal ordering process, to ensure they are taking advantage of the latest security measures incorporated into the product and in order to be ready to accept Patch Updates. Nortel strongly recommends upgrading to the latest release of SRG software to reduce potential security exposures.

Survivable Remote Gateway 50 - SRG50, SRG50b 2.0, SRG50b 3.0, SRG50 2.0, SRG50 3.0,

. The Linux BCM-based SRG50 product perform as expected and is not adversely impacted when subjected to the potential Sockstress TCP DoS (Outpost24 TCP Issues).

VPN Gateway - 3050, 3070

. While under heavy attack, NVG3050 and NVG3070 is still able to accept new SSL VPN connections

**Attachments:**

There are no attachments for this bulletin

**Products and Releases:**

The information in this bulletin is intended to be used with the following products and associated releases:

PRODUCT	RELEASE
BCM-BCM-BCM1000 Global	
BCM-BCM-BCM1000 N.A.	
BCM-BCM-BCM200 Global	
BCM-BCM-BCM200 N.A.	
BCM-BCM-BCM400 Global	
BCM-BCM-BCM400 N.A.	

BCM-BCM-BCM450 R1	
BCM-BCM-BCM50 Global	
BCM-BCM-BCM50 N.A.	
BCM-BCM-BCM50 R2 Global	
BCM-BCM-BCM50 R2 N.A.	
BCM-BCM-BCM50 R3 Global	
BCM-BCM-BCM50 R3 N.A.	
BCM-BCM-BCM50a Global	
BCM-BCM-BCM50a N.A.	
BCM-BCM-BCM50a R2 Global	
BCM-BCM-BCM50a R2 N.A.	
BCM-BCM-BCM50a R3 Global	
BCM-BCM-BCM50a R3 N.A.	
BCM-BCM-BCM50b R2 Global	
BCM-BCM-BCM50b R3 Global	
BCM-BCM-BCM50ba R2 Global	
BCM-BCM-BCM50ba R3 Global	
BCM-BCM-BCM50be R2 Global	
BCM-BCM-BCM50be R3 Global	
BCM-BCM-SRG200 1.0 Global	
BCM-BCM-SRG200 1.0 N.A.	
BCM-BCM-SRG200 1.5 Global	
BCM-BCM-SRG200 1.5 N.A.	
BCM-BCM-SRG400 1.0 Global	
BCM-BCM-SRG400 1.0 N.A.	
BCM-BCM-SRG400 1.5 Global	
BCM-BCM-SRG400 1.5 N.A.	
BCM-BCM-SRG50 2.0 Global	
BCM-BCM-SRG50 2.0 N.A.	
BCM-BCM-SRG50 3.0 Global	
BCM-BCM-SRG50 3.0 N.A.	
BCM-BCM-SRG50 Global	
BCM-BCM-SRG50 N.A.	
BCM-BCM-SRG50b 2.0 Global	
BCM-BCM-SRG50b 3.0 Global	
CallPilot-CallPilot-CallPilot 1002rp	
CallPilot-CallPilot-CallPilot 1005r	
CallPilot-CallPilot-CallPilot 201i	
CallPilot-CallPilot-CallPilot 202i	

CallPilot-CallPilot-CallPilot 600r	
CallPilot-CallPilot-CallPilot 703t	
Contact Center-Administration-Agent Desktop Display	
Contact Center-Applications-Agent Greeting	
Contact Center-Administration-CCMA	
Contact Center-Manager-CCMS	
Contact Center-CTI-CCT	
Contact Center-Manager-Contact Center - Express	
Contact Center-Multimedia-Contact Center - Multimedia	
Contact Center-Multimedia-Contact Center - Outbound	
Contact Center-Manager-NCC	
Contact Center-Applications-Remote Agent Observe	
Contact Center-CTI-Symposium Agent	
Contact Center-CTI-TAPI Server	
ENSM-NMS-Enterprise NMS	
Enterprise VoIP-Applications-TM-CS1000	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 5000-Ethernet Rtnng Swt 5650TD	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 8600-Ethernet Rtnng Switch 8600	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 2500-Ethernet Rtnng Swt 2526T	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 2500-Ethernet Rtnng Swt 2526T-PWR	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 3000-Ethernet Rtnng Swt 3510-24T	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 4500-Ethernet Rtnng Swt 4524GT	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 4500-Ethernet Rtnng Swt 4526FX	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 4500-Ethernet Rtnng Swt 4526G-PWR	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 4500-Ethernet Rtnng Swt 4526GTX	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 4500-Ethernet Rtnng Swt 4526T	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 4500-Ethernet Rtnng Swt 4526T-PWR	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 4500-Ethernet Rtnng Swt 4550T	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 5000-Ethernet Rtnng Swt 5510-24T	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 5000-Ethernet Rtnng Swt 5510-48T	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 5000-Ethernet Rtnng Swt 5698TFD	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 4500-Ethernet Rtnng Swt4524GT-PWR	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 4500-Ethernet Rtnng Swt4548GT-PWR	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 5000-Ethernet Rtnng Swt5530-24TFD	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 5000-Ethrnt Rtnng Swt5650TD-PWR	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 5000-Ethrnt Rtnng Swt5698TFD-PWR	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 2500-Ethrnt Rtnng Swt 2550T	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 2500-Ethrnt Rtnng Swt 2550T-PWR	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 4500-Ethrnt Rtnng Swt 4548GT	

Ethernet Rtnng Switch-Ethrnt Rtnng Swt 4500-Ethrnt Rtnng Swt 4550T-PWR	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 5000-Ethrnt Rtnng Swt5520-24T PWR	
Ethernet Rtnng Switch-Ethrnt Rtnng Swt 5000-Ethrnt Rtnng Swt5520-48T PWR	
Ethernet Switch-BPS 2000-Business Policy Switch 2000	
Ethernet Switch-325-Ethernet Switch 325-24G	
Ethernet Switch-325-Ethernet Switch 325-24T	
Ethernet Switch-380-Ethernet Switch 380-24T	
Ethernet Switch-400-Ethernet Switch 420-24T	
Ethernet Switch-400-Ethernet Switch 425-24T	
Ethernet Switch-400-Ethernet Switch 425-48T	
Ethernet Switch-460-Ethernet Switch 460-24T PWR	
Ethernet Switch-470-Ethernet Switch 470-24T	
Ethernet Switch-470-Ethernet Switch 470-48T	
Meridian-Messaging-MSM Mail System	
Meridian-Messaging-Meridian Mail Compact Opt.	
Meridian-Messaging-Meridian Mail EC11	
Meridian-Messaging-Meridian Mail MP	
Meridian-Messaging-Meridian Mail Mod. Option	
Meridian-Messaging-Meridian Mail Modular EC	
Meridian-Messaging-Meridian Mail Modular GP	
Meridian-Messaging-Meridian Mail NT/XT	
Meridian-Messaging-Meridian Option 11 Mail	
Multimedia Comm.-Applications-MAS	
Norstar-Core-3X8	
Norstar-Core-CICS	
Norstar-Messaging-Desktop Messaging	
Norstar-Messaging-Flash ACD	
Norstar-Core-MICS	
Norstar-Messaging-NVM Manager	
Norstar-Peripherals-Norstar VoIP Gateway	
Norstar-Applications-PC Console	
Norstar-Applications-Personal Productivity Suite	
Secure Ntwk Access-Identity Engines-Identity Eng Igntn Analctcs	
Secure Ntwk Access-Identity Engines-Identity Eng Igntn Gst Mgr	
Secure Ntwk Access-Identity Engines-Identity Eng Igntn Pstr	
Secure Ntwk Access-Identity Engines-Identity Eng Igntn Srvr	
Secure Ntwk Access-Switch 4000-Secure Ntwk Access Swt 4050	
Secure Ntwk Access-Switch 4000-Secure Ntwk Access Swt 4070	
Self-Service-Self-Service-CCSS7	

Self-Service-Web Centric Self-Svc-CCXML	
Self-Service-Packaged Application-CDD	
Self-Service-Media Processing Svr-Media Processing Svr 100	
Self-Service-Media Processing Svr-Media Processing Svr 1000	
Self-Service-Media Processing Svr-Media Processing Svr 500	
Self-Service-Self-Service-Peri Application	
Self-Service-Self-Service-Peri CTI	
Self-Service-Self-Service-Peri IVR	
Self-Service-Self-Service-Peri NT Server	
Self-Service-Self-Service-Peri Workstation	
Self-Service-Self-Service-Speech Server	
Self-Service-Application Center-Video Server	
Self-Service-Web Centric Self-Svc-VoiceXML	
Self-Service-Web Centric Self-Svc-WVADS	
Switched Firewall-Switched Firewall-SF-5109	
Switched Firewall-Switched Firewall-SF-5114	
Switched Firewall-Switched Firewall-SF/VPN 5124	
Switched Firewall-Switched Firewall-SFA-6400	
Switched Firewall-Switched Firewall-SFA-6600	
VPN Gateway-VPN Gateway-VPN 3050	
VPN Gateway-VPN Gateway-VPN 3070	

To view the most recent version of this bulletin, access technical documentation, search our knowledge base, or to contact a Technical Support Representative, please visit Nortel Technical Support on the web at: <http://support.nortel.com/>. You may also sign up to receive automatic email alerts when new bulletins are published.

**REFERENCE:** CVE-2008-4609  
**PRE-REQUIRED PATCH:**  
**PATCH ID:**

Copyright 2009 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel assumes no responsibility for any errors that may appear in this document. The information in this document is proprietary to Nortel Networks.

Nortel recommends any maintenance activities, such as those outlined in this bulletin, be completed during a local maintenance window.

Nortel, the Nortel logo, and the Globemark design are trademarks of Nortel Networks. All other trademarks are the property of their respective owners.