NORTEL

>TECHNICAL SUPPORT
SECURITY ADVISORY BULLETIN

Nortel Enterprise Response to VU#261869: Clientless SSL VPN Security Issue

Source:

US-CERT Vulnerability Note on the Clientless SSL VPN Security Issues at: http://www.kb.cert.org/vuls/id/261869
CVE-2009-2631 at: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2631
CERT- Coordination Center CA-200-02 is available at: http://www.cert.org/advisories/CA-2000-02.html#impact

BULLETIN ID: 2009009920, Rev 1
PUBLISHED: 2009-12-15
STATUS: Active
REGION: All
PRIORITY: Critical
TYPE: Security Advisory

Overview:

Clientless SSL VPN products from multiple vendors operate in a way that breaks fundamental browser security mechanisms. An attacker could use these devices to bypass authentication or conduct other web-based attacks.

By convincing a user to view a specially crafted web page, a remote attacker may be able to obtain VPN session tokens and read or modify content (including cookies, script, or HTML content) from any site accessed through the clientless SSL VPN. This effectively eliminates same origin policy restrictions in all browsers. Because all content runs at the privilege level of the web VPN domain, mechanisms to provide domain-based content restrictions, such as Internet Explorer security zones and the Firefox add-on NoScript, may be bypassed. For example, the attacker may be able to capture keystrokes while a user is interacting with a web page. For additional information about impacts, please review CERT Advisory CA-2000-02.

There is no solution to this problem. Depending on their specific configuration and location in the network these devices may be impossible to operate securely. Administrators are encouraged to view the workarounds detailed in the Solutions section of the US-CERT Vulnerability Note for the following:

1. Limit URL rewriting to trusted domains

2. Block the VPN server from accessing untrusted domains

3. Disable URL hiding features

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

Risk:
Please refer to the US-CERT link in the Source section for additional information about the risks of the various vulnerabilities addressed by the US-CERT 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 US-CERT Advisory for Clientless SSL VPN Security Issues. Please refer to product-specific text below for instructions on how to proceed.

CallPilot - 201i, 202i, 600r, 703t, 1002rp, 1005r
. Customers should avoid browsing other web sites while logged in securely to CallPilot Manager or My CallPilot.

2) The following Nortel Generally Available products are not vulnerable to the security issue outlined in the US-CERT Advisory for Clientless SSL VPN Security Issues. Please refer to product-specific information below for any further instructions.

BCM - BCM50, BCM200, BCM400, BCM450, BCM1000, SRG50, SRG200, SRG400
. The BCM and BCM-based SRG is not impacted by Clientless SSL VPN products that break web browser's domain-based security models issue, as the BCM / SRG models do not have a clientless SSL VPN solution.

Contact Center - CCT
. Contact Center portfolio products have no dependency on any affected Clientless SSL VPN products and the vulnerability is not applicable to any Contact Center portfolio products.

Contact Center - Agent Greeting
. Contact Center portfolio products have no dependency on any affected Clientless SSL VPN products and the vulnerability is not applicable to any Contact Center portfolio products.

Contact Center - Contact Recording, Quality Monitoring
. Contact Center portfolio products have no dependency on any affected Clientless SSL VPN products and the vulnerability is not applicable to any Contact Center portfolio products.

Contact Center - Multimedia Agent Desktop Display, CCMM, Outbound
. Contact Center portfolio products have no dependency on any affected Clientless SSL VPN products and the vulnerability is not applicable to any Contact Center portfolio products.

Contact Center - Manager CCMA, CCMS, Express, NCC
. Contact Center portfolio products have no dependency on any affected Clientless SSL VPN products and the vulnerability is not applicable to any Contact Center portfolio products.

Contact Center - Remote Agent Observe
. Contact Center portfolio products have no dependency on any affected Clientless SSL VPN products and the vulnerability is not applicable to any Contact Center portfolio products.

Call Center - Symposium Agent, TAPI Server
. Contact Center portfolio products have no dependency on any affected Clientless SSL VPN products and the vulnerability is not applicable to any Contact Center portfolio products.

ENSM - Configuration & Orchestration Manager (COM)
. This issue is not product specific (COM) and impacts all web applications. We recommend the remediation workaround for how to manage your SSL VPN to overcome or limit this issue.

Enterprise NMS - ENMS
. ENMS application is not truly a browser based application though it can be accessed as an applet in the browser. Nortel recommends users to access ENMS as the desktop or Java client level - i.e. not to use the applet version.

Enterprise VoIP - TM-CS1000
. TM is not impacted by the Clientless SSL VPN products break web browser's domain-based security models, as this is not applicable to TM. Customers may choose to follow the potential workarounds as published by US-CERT.

Enterprise VoIP - CS1000M, CS1000S
. The CS1000 is not impacted by the Clientless SSL VPN products break web browser's domain-based security models, because it does not use any clientless SSL.

Ethernet Routing Switch - 1424, 1612, 1624, 1648
. The product does not offer an SSL VPN service

Ethernet Routing Switch - 55xx, 56xx
. There is no solution for this problem on 5600 itself. Customer may implement the mitigating solutions as per the US-CERT Notification.

Ethernet Routing Switch - 8300, 8600, 8661
. By design, the backend session cookie is maintained on the VPN Gateway and is not exposed to the user side of the connection.

VPN Gateway - 3050, 3070
. By design, the backend session cookie is maintained on the VPN Gateway and is not exposed to the user side of the connection.

Messaging - MSM 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
. Meridian Mail does not use browsers, web servers or SSL

Norstar Applications - PC Console, Personal Productivity Suite
. Clientless SSL is not used on any Norstar products. Hence, the Norstar KSUs and Norstar applications are not affected by the Clientless SSL VPN products break web browser's domain-based security models potential vulnerability.

Norstar Core - 3X8, CICS, MICS
. Clientless SSL is not used on any Norstar products. Hence, the Norstar KSUs and Norstar applications are not affected by the Clientless SSL VPN products break web browser's domain-based security models potential vulnerability.

Norstar Messaging - Desktop Messaging, Flash ACD, Norstar Voice Mail
. Clientless SSL is not used on any Norstar products. Hence, the Norstar KSUs and Norstar applications are not affected by the Clientless SSL VPN products break web browser's domain-based security models potential vulnerability.

Norstar Peripherals - Norstar VoIP Gateway
. Clientless SSL is not used on any Norstar products. Hence, the Norstar KSUs and Norstar applications are not affected by the Clientless SSL VPN products break web browser's domain-based security models potential vulnerability.

Secure Network Access - Identity Engines Ignition Analytics, Identity Engines Ignition Guest Manager, Identity Engines Ignition Posture, Identity Engines Ignition Server
. NIEIS is not vulnerable to this issue because there is no Captive Portal in the portfolio to perform URL re-write.

Secure Network Access Switch - 4050, 4070
. NSNA is not vulnerable to this issue since it does not perform re-write of the URLS and does not use a globally unique cookie method as well; the site cookies are not exposed outside of the code

Secure Router - 1001, 1002, 1004, 2330, 3120, 4134, 8002, 8004, 8008, 8012
. The product does not offer an SSL VPN service

VPN Router - VPN Client
. Nortel VPN Client is not browser based.

VPN Router - 600, 1010, 1050, 1100, 1700, 1740, 1750, 2700, 2750, 5000, Contivity 2600, Contivity 4500, Contivity 4600
. SSL is used to securely configure the device only. A device manager has to provide a username and password to establish the connection; this authentication allows management access (privileged access) to the whole device; the VPN Router (server) then sends a cookie to the browser; changing a cookie will not result in any adverse operation (gaining more privileges than before or automatic redirection to another device/service). There is no solution for this problem on a VPN Router itself. Customer may implement a network-based mitigating solution as per the US-CERT advisory.

WLAN - Management System, Management Software
. This product does not support this Clientless SSL VPN

WLAN Mobile Adapter - 2201, 2202
. This product does not support this Clientless SSL VPN

WLAN Access Point - 2330, 2332
. WLAN Access Point 2300 does not support Clientless SSL VPN.

WLAN Security Switch - 2350, 2360, 2361, 2380, 2382, Location Engine 2340
. This product does not support this Clientless SSL VPN

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-BCM50e Global	
BCM-BCM-BCM50e N.A.	
BCM-BCM-BCM50e R2 Global	
BCM-BCM-BCM50e R2 N.A.	
BCM-BCM-BCM50e R3 Global	
BCM-BCM-BCM50e R3 N.A.	
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-Monitoring-Contact Recording	
Contact Center-Manager-NCC	
Contact Center-Monitoring-Quality Monitoring	
Contact Center-Applications-Remote Agent Observe	
Contact Center-CTI-Symposium Agent	
Contact Center-CTI-TAPI Server	
ENSM-COM-COM	
ENSM-NMS-Enterprise NMS	
Enterprise VoIP-Core-CS 1000M Chassis/Cabinet	
Enterprise VoIP-Core-CS 1000M Half Group	
Enterprise VoIP-Core-CS 1000M Multi Group	
Enterprise VoIP-Core-CS 1000M Single Group	
Enterprise VoIP-Core-CS 1000S	
Enterprise VoIP-Applications-TM-CS1000	
Ethernet Rtng Switch-Ethrnt Rtng Swt 1000-Ethernet Routing Switch1424	
Ethernet Rtng Switch-Ethrnt Rtng Swt 1000-Ethernet Routing Switch1612	
Ethernet Rtng Switch-Ethrnt Rtng Swt 1000-Ethernet Routing Switch1624	
Ethernet Rtng Switch-Ethrnt Rtng Swt 1000-Ethernet Routing Switch1648	
Ethernet Rtng Switch-Ethrnt Rtng Swt 5000-Ethernet Rtg Swt 5650TD	
Ethernet Rtng Switch-Ethrnt Rtng Swt 8300-Ethernet Rtng Switch 8306	
Ethernet Rtng Switch-Ethrnt Rtng Swt 8300-Ethernet Rtng Switch 8308XL	
Ethernet Rtng Switch-Ethrnt Rtng Swt 8300-Ethernet Rtng Switch 8310	
Ethernet Rtng Switch-Ethrnt Rtng Swt 8300-Ethernet Rtng Switch 8348GB	
Ethernet Rtng Switch-Ethrnt Rtng Swt 8300-Ethernet Rtng Switch 8348TX	

Ethernet Rtng Switch-Ethrnt Rtng Swt 8300-Ethernet Rtng Switch 8393SF	
Ethernet Rtng Switch-Ethrnt Rtng Swt 8300-Ethernet Rtng Switch 8394SF	
Ethernet Rtng Switch-Ethrnt Rtng Swt 8600-Ethernet Rtng Switch 8600	
Ethernet Rtng Switch-Ethrnt Rtng Swt 8600-Ethernet Rtng Switch 8661	
Ethernet Rtng Switch-Ethrnt Rtng Swt 8300-Ethernet Rtng Switch8324GTX	
Ethernet Rtng Switch-Ethrnt Rtng Swt 8300-Ethernet Rtng Switch8348GTX	
Ethernet Rtng Switch-Ethrnt Rtng Swt 5000-Ethernet Rtng Swt 5510-24T	
Ethernet Rtng Switch-Ethrnt Rtng Swt 5000-Ethernet Rtng Swt 5510-48T	
Ethernet Rtng Switch-Ethrnt Rtng Swt 5000-Ethernet Rtng Swt 5632FD	
Ethernet Rtng Switch-Ethrnt Rtng Swt 5000-Ethernet Rtng Swt 5698TFD	
Ethernet Rtng Switch-Ethrnt Rtng Swt 5000-Ethernet Rtng Swt5530-24TFD	
Ethernet Rtng Switch-Ethrnt Rtng Swt 5000-Ethrnt Rtg Swt5650TD-PWR	
Ethernet Rtng Switch-Ethrnt Rtng Swt 5000-Ethrnt Rtg Swt5698TFD-PWR	
Ethernet Rtng Switch-Ethrnt Rtng Swt 5000-Ethrnt Rtng Swt5520-24T PWR	
Ethernet Rtng Switch-Ethrnt Rtng Swt 5000-Ethrnt Rtng Swt5520-48T PWR	
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	
Mltsvc Access Switch-4400-Mltsrvc Acc Switch 4460	
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	
Phones & Accessories-Wireless-WLAN Appl. Gateway 2246	
Secure Ntwk Access-Identity Engines-Identity Eng Igntn Analtcs	
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	
Secure Router-1000-Secure Router 1001	
Secure Router-1000-Secure Router 1002	
Secure Router-1000-Secure Router 1004	
Secure Router-2000-Secure Router 2330	
Secure Router-3100-Secure Router 3120	
Secure Router-4100-Secure Router 4134	
Secure Router-8000-Secure Router 8002	
Secure Router-8000-Secure Router 8004	
Secure Router-8000-Secure Router 8008	
Secure Router-8000-Secure Router 8012	
VPN Gateway-VPN Gateway-VPN 3050	
VPN Gateway-VPN Gateway-VPN 3070	
VPN Router-2000-Contivity 2600	
VPN Router-4000-Contivity 4500	
VPN Router-4000-Contivity 4600	
VPN Router-Client-VPN Client	
VPN Router-1000-VPN Router 1010	
VPN Router-1000-VPN Router 1050	
VPN Router-1000-VPN Router 1100	
VPN Router-1000-VPN Router 1700	
VPN Router-1000-VPN Router 1740	
VPN Router-1000-VPN Router 1750	
VPN Router-2000-VPN Router 2700	
VPN Router-2000-VPN Router 2750	
VPN Router-5000-VPN Router 5000	
VPN Router-600-VPN Router 600	
WLAN-2300-WLAN Access Point 2330	
WLAN-2300-WLAN Access Point 2332	
WLAN-2300-WLAN Location Engine 2340	
WLAN-2300-WLAN Management Software	
WLAN-2200-WLAN Management System	
WLAN-2200-WLAN Mobile Adapter 2201	
WLAN-2200-WLAN Mobile Adapter 2202	
WLAN-2300-WLAN Security Switch 2350	
WLAN-2300-WLAN Security Switch 2360	
WLAN-2300-WLAN Security Switch 2361	
WLAN-2300-WLAN Security Switch 2380	

WLAN-2300-WLAN Security Switch 2382	

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: VU#261869
PRE-REQUIRED PATCH:
PATCH ID:

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