Bulletin Identification Number:
DB022002-1

Issue:
3

Type:
Warning

Priority:
Critical

Software ID:

CVX Software Loads that Currently Include an Update for SNMP Issues Highlighted by CERT.			
CVX 1800/CVX 600			**CVX 1800 VOIP**
Version 3	**Version 4**	**Version 5**	**Version 200**
3.6.3P25	4.1P6	5.0.1P2	CV200P6
	4.2P8	5.1	
	4.3	5.2	
	4.4		

Other References:
SNMP CERT Advisory CA-2002-03 ("SNMP Advisory"),
Nortel Networks Portfolio Summary in response to CERT SNMP Vulnerabilities Advisory CA-2002-03 ("Nortel Networks Portfolio Summary"), and Nortel Networks Best Practices at http://www.nortelnetworks.com/corporate/technology/snpmv1.html ("Best Practices").

Title:
CVX Response to CERT SNMP Advisory

Description: Platform impact resulting from testing with the CERT PROTOS c06-snmpv1 test suite ("Test Suite").

On February 12, 2002 CERT/CC issued the SNMP advisory to the public that contained two vulnerability notes (VU#107186 and VU#854306).

VU#107186 - Multiple vulnerabilities in SNMPv1 trap handling

VU#854306 - Multiple Vulnerabilities in SNMPv1 request handling

Impact:
When the CVX platform is subjected to the Test Suite the platform is impacted as a result of the issues described in the SNMP Advisory and will result in the system not functioning. All current

users will be disconnected and the CVX will auto-recover and return to service in approximately 5 minutes. The exact time of recovery will depend on the number of ports installed and configured.

Solution:
Nortel Networks issued software code updates to eliminate the SNMP vulnerability as highlighted by CERT. The software code updates are listed in the table in the **Software ID** section at the beginning of this document. If you are unsure what version of code is currently installed on your CVX platform please issue the vinfo command at the CVX prompt. If an upgrade is required please contact your local support organization as soon as possible for assistance in obtaining the appropriate version. If an immediate upgrade is not possible please follow the steps listed in the **Recommendation** section below.

Recommendation:
Nortel Networks does not recommend executing the CERT/CC Test Suite in a production environment. The packets contained in the Test Suite have abnormalities and should only be run in a lab environment.

Implement private network LAN or Ingress filtering, as recommended in the Nortel Networks Portfolio Summary and Best Practices. If unable to implement private network LAN or Ingress filtering, as recommended in the Nortel Networks Portfolio Summary, the **immediate** mitigating factor recommended is to disable SNMP on the CVX platform.

Once SNMP is turned off, the CVX will no longer be impacted by these specific potential SNMP vulnerabilities described in the SNMP Advisory.

The method used to disable SNMP on the CVX platform is as follows:

From the CVX command line interface issue the type config.cvx command so that you will have a picture of the non-default containers and/or parameters configured. Please look for the following items under the system container. If a container does not show up or parameters within the container do not show up that does not mean they are not present or not active.

For instance, ip_snmp may not show up in the configuration but may be active and be using its default settings. This means that the ip_snmp container is enabled by default. Therefore, the read_community and write community strings should be changed from their default values of public and private respectively for obvious security reasons. It is important to note that altering these strings will affect the ability to manage the CVX unless appropriate changes are made to other devices within the management network. Also filtering may be done on inbound UDP ports 161 and 162 which are also described in this section below.

```
(Sample container for ip_snmp)
configure ip_snmp
    debug_flag 1
    log_flag 2
    read_community <value obfuscated>
    write_enabled true (Default value that would not be seen when viewing typed config.)
    write_community <value obfuscated>
    max_snmp_load 100  (Default value that would not be seen when viewing typed config.)
    commit
```

The traps container should be removed from the config. This can be accomplished in the CLI via the delete command. Enter the config mode and type the following commands (in italics).

```
config
configure system/ip_services/ip_service
system/ip_services/ip_service>delete ip_traps
```

```
Deleting an item is an irreversible process.
Are you sure you want to delete this item? [Y/N]Y
```

(Sample container for ip_traps)

```
configure ip_traps
        configure ip_trap_cfg 1  (There may be one or more trap servers configured)
          set priority info
          set ip_addr 10.1.0.96
          commit
```

The ip_svc_entry container should be checked to see if there is an entry enabling the snmp_server service. This service should be disabled in the config. This can be accomplished in the CLI via the following path. Enter the config mode and type the following commands (in italics).

```
config
configure system/ip_services/ip_service/ip_svc_entry 1
.../ip_services/ip_service/ip_svc_entry 1>show
  Members currently configured at this level:
    service snmp_server
    admin_status enabled
    restricted false
.../ip_services/ip_service/ip_svc_entry 1>set admin_status disabled
.../ip_services/ip_service/ip_svc_entry 1>commit
```

(Sample container for ip_svc_entry)

```
configure ip_svc_entry 1
       set service snmp_server
       admin_status disabled (Default value is enabled and should be disabled for this
bulletin)
       commit
```

The session_config container should be checked to see if the SNMP disconnect parameter has been enabled. This allows user sessions to be disconnected via SNMP and should be set to false if not in use. This can be disabled using the following commands (in italics).

```
Config
Configure sessions/session_config
Sessions/session_config>show
  Members currently configured at this level:
    DefaultVpopEnable true
    PreAuth radius
    PreAuthPassword <value obfuscated>
    PreAuthTimeout 4
    PreAuthTimeoutAction accept
    CheckpointTime 0
    terminateEnable disabled
    terminateSecret <value obfuscated>
    logEnable true
    PreAuthAAAGroup 1
    DS0DiscTimeOut 120
    acctReportFailedSessions false
    RealAuthDisable false
    snmpDisconnectEnable true
sessions/session_config>set snmpdisconnectenable false
sessions/session_config>commit
```

(Sample container for session_cfg)

```
  configure session_config
    set PreAuth radius
    set PreAuthPassword PW1/7jWat9Y
    set PreAuthTimeout 4
    set PreAuthAAAGroup 1
    set snmpDisconnectEnable true(Default value for this parameter false should be used.)
    commit
```

The following text describes one method of implementing an access list to eliminate all SNMP traffic in-bound to the CVX. Note this will disable the CVX from receiving all management SNMP traffic on UDP ports 161 and 162. (UDP ports 161 and 162 are the well-known standard SNMP ports utilized by the CVX.)

The first step is to configure three ip_access_lists under the ip_router container on the CVX. The first access list blocks traffic destined for UDP port 161, the second blocks traffic destined for port 162, and the third allows all other traffic. The third entry is necessary because the first access list implemented will also implicitly deny all other traffic from reaching the CVX. Note: The access list numbers, 500, 501, and 502 are user-defined numbers that were chosen for this example.

```
...system/ip_router/ip_access_list 500>show
  Members currently configured at this level:
    id 500
    mode deny
    protocol udp
    source_ip 0.0.0.0    ← All traffic form source_ip 0.0.0.0 will be denied


source_mask 0.0.0.0  ← All traffic form source_mask 0.0.0.0 will be denied
    destination_ip 0.0.0.0 ← All traffic to destination_ip 0.0.0.0 will be denied
    destination_mask 0.0.0.0 ← All traffic to destination_mask 0.0.0.0 will be denied
    compare eq
    destination_port 161
    icmp_type 0
    icmp_code 0
    igmp_type 0
    tcp_flag none
...system/ip_router/ip_access_list 500>

system/ip_router>configure ip_access_list 501
...system/ip_router/ip_access_list 501>show
  Members currently configured at this level:
    id 500
    mode deny
    protocol udp
    source_ip 0.0.0.0  ← All traffic form source_ip 0.0.0.0 will be denied
    source_mask 0.0.0.0 ← All traffic form source_mask 0.0.0.0 will be denied
    destination_ip 0.0.0.0 ← All traffic to destination_ip 0.0.0.0 will be denied
    destination_mask 0.0.0.0 ← All traffic to destination_mask 0.0.0.0 will be denied
    compare eq
    destination_port 162
    icmp_type 0
    icmp_code 0
    igmp_type 0
    tcp_flag none
...system/ip_router/ip_access_list 501>

system/ip_router>configure ip_access_list 502
...system/ip_router/ip_access_list 502>show
  Members currently configured at this level:
    id 500
    mode permit
    protocol any
    source_ip 0.0.0.0
    source_mask 0.0.0.0
    destination_ip 0.0.0.0
    destination_mask 0.0.0.0
    compare none
    destination_port 0
    icmp_type 0
    icmp_code 0
    igmp_type 0
    tcp_flag none
```

The next step is to configure an ip access group for each ethernet interface in the CVX as shown below. Note: The access list group number 500 is a user-defined number that was chosen for this example.

```
FEP> config shelf 1/
Entering Configuration Mode
shelf 1>configure slot 9
shelf 1/slot 9>configure scc/bic
shelf 1/slot 9/SCC/BIC>configure ethernet 1
.../SCC/BIC/Ethernet 1>configure ip_interface
.../BIC/Ethernet 1/ip_interface>configure ip_access_group 500
.../Ethernet 1/ip_interface/ip_access_group 500>show
  Members currently configured at this level:
    if_index 1
    access_list_id 500
    direction in
.../Ethernet 1/ip_interface/ip_access_group 500>
```

Notes:

Retirement Action:
Content to be reviewed or retired January 2003.

For Additional Information:
CONTACT YOUR LOCAL SUPPORT ORGANIZATION. Express Routing Code 832