

[UNIX] Linux NetFilter NAT/ICMP Code Information Leak

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0059.html>

From: support@securiteam.com

Date: 05/12/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 12 May 2002 14:58:40 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Linux NetFilter NAT/ICMP Code Information Leak

SUMMARY

The following bug exists in the NetFilter NAT implementation: When the first packet of a connection is hitting a NAT rule, and this packet causes the NAT box itself to reply with an ICMP error message, the inner IP packet inside the ICMP error message is not un-NAT'ed correctly. This leads to the ability to discover which ports of a host are NATed and where the packet will really go. This can also lead to those ICMP error packets being dropped by "stateful" firewalls not recognizing the related connection.

DETAILS

Vulnerable versions:

* All kernel patches from IPTables package < ipables-1.2.6a are vulnerable.

* All versions of kernel >= 2.4.4 and up to (at least) 2.4.19-pre6 use a vulnerable version.

Vendor status:

The NetFilter team has solved this bug with a patch that has been refused for inclusion in the Linux kernel. They are working on a new patch.

Securiteam: [UNIX] Linux NetFilter NAT/ICMP Code Information Leak

Solutions:

- * Upgrade your kernel using the patch at <http://www.netfilter.org/security/2002-04-02-icmp-dnat.html> (link active starting with May 8) or http://www.cartel-securite.fr/pbiondi/2.4.19-pre6_icmp-nat.patch
- * Use a workaround until the final solution to this bug is implemented and included in the Linux kernel source.

Workarounds:

Filter out untracked local packets:

```
iptables -A OUTPUT -m state -p icmp --state INVALID -j DROP
```

Example:

Let us take a machine (172.16.1.40) that DNAT port 666 to 172.16.3.26:22 :

```
iptables -t nat -A PREROUTING -p tcp --dport 666 -j DNAT --to 172.16.3.26:22
```

Then if a host sends a packet that will die on 172.16.1.40 :

```
hping -t 1 --syn -p 666 172.16.1.40
```

This is the icmp packet we'll get from 172.16.1.40 :

```
17:07:46.709230 172.16.1.40 > 172.16.1.28: icmp: time exceeded in-transit
0x0000 45c0 0044 eaa6 0000 ff01 75f1 ac10 0128 E..D.....u....(
0x0010 ac10 0118
          0b00 516d 0000 0000
                    4500 0028 .....Qm....E..(
0x0020 b0f3 0000 0106 ac8a ac10 0118 ac10 031a <-+ .....
0x0030 04bd 0016 3206 3ec0 0490 00b4 5002 0200 | ....2.>.....P...
0x0040 d6b2 00^0 | ....
          | 172.16.3.26
          +-- port 22
```

You can also try a patch to nmap that does that and much more:

<http://www.cartel-securite.fr/pbiondi/nmap/>

```
# ./nmap -sS -P0 xxx.xxx.xxx.xxx -p 22,23,666,667 -t 9
```

Starting nmap V. 2.54BETA32 (www.insecure.org/nmap/)

Interesting ports on xxx.xxx.xxx.xxx:

Port State Service

22/tcp open ssh

23/tcp filtered telnet

666/tcp UNfiltered unknown DNAT to 192.168.8.10:22

667/tcp UNfiltered unknown DNAT to 192.168.26.10:22

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds.

ADDITIONAL INFORMATION

Securiteam: [UNIX] Linux NetFilter NAT/ICMP Code Information Leak

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:

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] Critical Path inJoin Directory Server Web Traversal Issue"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)