

Re: Linux kernel 2.4 "weak end host" issue Explained

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-05/0123.html>

From: Matthew G. Marsh (mgm@paktronix.com)

Date: 05/14/02

Date: Tue, 14 May 2002 09:47:22 -0500 (CDT)
From: "Matthew G. Marsh" <mgm@paktronix.com>
To: bugtraq@securityfocus.com

Note to Moderator: I can provide a more detailed explanation for the commands cited below but feel it may not be of interest to the broader public. If you would prefer.

On Thu, 9 May 2002, Felix von Leitner wrote:

- > *A service bound to the IP of eth1 is still visible from eth0.*
- > *This is not an RFC violation (RFC1122 calls this "weak end host"), but*
- > *it is unexpected for most Linux users, and the very reason why people*
- > *bind a service to the IP of a specific network interface usually is to*
- > *make sure it can only be used from that interface (DHCP, samba, squid*
- > *and intranet web servers come to mind).*

Any Linux users who think this way are sadly misinformed as to how IPv4 works in general. This is expected and normal behaviour for Linux. Stating otherwise reveals a deep disregard for the variety of structure and definition of IPv4 and an assumption that there is only one true way. Bluntly put – the world is not BSD nor is it Microsoft. Read the RFCs and learn how IPv4 works.

IP addresses have nothing to do with physical interfaces. An IP address (or indeed any generalized location structure name) defines the contact point for a service. All references to binding exist due to this fundamental fact of addressing. That is why ARP exists in the first place. ARP is a protocol to allow communication over Layer 2 (DataLink) to occur as required (think raw ethernet/token ring) between a Service and Requestor.

- > *This is not an ARP issue. Making the kernel stop answering to ARP*
- > *requests will not make it harder for an attacker to reach the service.*

Correct. [snip]

SecurityFocus Bugtraq: Re: Linux kernel 2.4 "weak end host" issue Explained

- > *There is a Linux*
- > *specific kludge^Whack^Wmethod to bind to an interface, but I am not*
- > *aware of any software using it. If you have multi homed hosts and rely*
- > *on a service bound to eth1 not being visible to eth0, you need to use*
- > *netfilter or this patch!*

No. Due to the unparalleled scope and breadth of Linux IPv4 networking you simply can change the behaviour through routing. Example:

```
eth0 = 1.1.1.1/24
eth1 = 2.2.2.2/24
```

```
ip rule add from 1.1.1.1/32 dev lo table 1 prio 15000
ip rule add from 2.2.2.2/32 dev lo table 2 prio 16000
```

```
ip route add default dev eth0 table 1
ip route add default dev eth1 table 2
```

If anyone would like more detailed explanations of this subject please feel free to email me. Linux IPv4 routing contains a wealth of power under the hood.

> *Felix*

Matthew G. Marsh, President
Paktronix Systems LLC
1506 North 59th Street
Omaha NE 68104
Phone: (402) 932-7250 x101
Email: mgm@paktronix.com
WWW: <http://www.paktronix.com>

- **Previous message:** [BrainRawt .: "LevCGI.coms NetPad 1.0.2 multiple vulnerabilities"](#)
- **In reply to:** [Felix von Leitner: "Linux kernel 2.4 "weak end host" issue \(previously discussed here as "arp problem"\)"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)