

Re: Martian Source

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2003-05/0003.html>

From: Seth Arnold (sarnold_at_wirex.com)

Date: 05/01/03

Date: Thu, 1 May 2003 10:22:12 -0700
To: "Javier Togra A." <jtogra@inocar.mil.ec>

On Wed, Apr 30, 2003 at 09:06:53AM -0500, Javier Togra A. wrote:
> *kernel: ll header: ff:ff:ff:ff:ff:ff:00:0a:04:b3:83:c0:08:06*
> *kernel: martian source 255.255.255.255 from 169.254.207.9, on dev eth0*
> *kernel: ll header: ff:ff:ff:ff:ff:ff:00:0a:04:b3:82:40:08:00*
> *kernel: martian source 169.254.207.9 from 169.254.207.9, on dev eth0*
>
> *Could some one tell me what does it mean, and what can I do ?*

martian packets are simply ones the kernel can easily tell are spoofed or otherwise incorrect.

You'll notice the first one has the source set to the local-net broadcast address -- obviously an incorrect packet. (When devices are attempting to discover their IP address, they use a source address of zeros and send to the local-net broadcast address.)

The second packet has a source address set to the IP address of the network interface that received the packet -- obviously an incorrect packet.

I'd classify these as "mostly harmless" -- if you have security problems that are remotely exploitable, chances are good the attacker already knows about them. If you don't have any remotely exploitable security problems, these are really nothing to be afraid of.

There isn't a lot you can do, aside from trace the linklevel header (reporting ethernet MAC pairs of source and destination, I don't recall in which order) and find the machine that is injecting these bad packets onto the network.

--

"Learning curve encryption is much more powerful than elliptical curve encryption." -- Alan Olsen

- application/pgp-signature attachment: [stored](#)