

Re: CR vs. CoreBuilder

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2001-08/0084.html>

From: randy (randy@eccs-com.net)

Date: 08/06/01

Date: Sun, 5 Aug 2001 20:46:24 -0700 (PDT)
From: randy <randy@eccs-com.net>
To: terry white <twhite@aniota.com>
Subject: Re: CR vs. CoreBuilder
Message-ID: <Pine.LNX.4.33.0108052029040.31346-100000@falcon.eccs-com.net>

On Sun, 5 Aug 2001, terry white wrote:

> on "8-5-2001" "John Nemeth" writ:
>
> : I have a 3Com CoreBuilder 3500 running software version 2.1.0 that
> : has been falling over a lot over the last few days.
>
> : NOTE: I don't have any proof that it is CodeRed that is causing the
> : CoreBuilder to fall over, but it is highly likely.
>
> ... i've noticed a similar problem with a cisco 675 ADSL router. in
> particular, i've had to do a cold boot three (3) times 'since' the CR-II
> attack started. i had disabled the web command interface, and checking
> revealed that still the case.
>
> what i did however, was to assign a port other than the default
> (sorry) of '80'. the device has been up 21 hours, despite an order of
> magnitude greater CR-II attempts. my server is not published, but in the
> last 5 days, i've seen 22, 25, 25, 47, and 60 (so far today: ~16:00 PDT)
> events ...

I have a very similar problem as well. I have a Cisco 675 and it has been crashing all weekened. I was running CBOS 2.20 and recently upgraded to 2.4.2 but it failed again after the upgrade. I have hit seven power cycles this weekend alone. I have also changed the port number to see if it makes any difference. It is a great suggestion. I tried a simple telnet to the router and noticed that even with the web interface disabled it still responds at the lower level. What I mean is that if the port number is set to 80 and I do a "telnet routeraddress 80" I get back a

```
Connected to routeraddress.  
Escape character is '^]'.  
Connection closed by foreign host.
```

SecurityFocus Bugtraq: Re: CR vs. CoreBuilder

But if I move the port the web interface is set to then the response on port 80 is different. It will just time out with no response at all.

A no