

Re: Rumours about Apache 1.3.22 exploits -> analysis of so-called exploit client

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-03/0068.html>

From: Sean Davis (dive@endersgame.net)

Date: 03/07/02

Date: Thu, 7 Mar 2002 00:07:31 -0500
From: Sean Davis <dive@endersgame.net>
To: adamb <adamb@twiki.iconideas.com>

First, I want to thank everybody who has posted information on this - it's something that (for obvious reasons) we don't want on our machines.

I have a question, however. Does this "virus" only affect Linux hosts? I personally do not run Linux, and have not for some time (all the security problems being just one of many reasons, but I don't want this to become an OS war)

I run NetBSD. NetBSD has, as an option. Linux binary emulation. Now, while I don't think there is any way for this virus to infect any other files on your system (that you do not own) unless you are root, how exactly is this program getting root?

Stop me if I'm wrong - but this thread was originally about apache exploits. Where is the vulnerability, apache, php, or what?

As the apache I run isn't highly used, I find it prudent to disable it until this issue is properly addressed by all vendors involved (Linux <whatever dist>, Apache, perhaps others), but obviously that's not acceptable for people who run web servers and such.

I think, and I may again be wrong, that this kind of thing could happen to NetBSD. That's why my reply is cc'd to tech-security: I want some sort of advice on just how worried I should be. Should I get rid of the linux compatibility?

Okay, enough with the rant section. Has anyone developed a program yet to scan a binary for the virus itself? strings, grep, etc, doesn't seem like the most elegant manner to scan a whole system's worth of binaries. Might take a while :-)

-Sean

On Wed, Mar 06, 2002 at 10:39:19PM -0500, adamb wrote:

> Well, thanks to my post earlier today, a fine person sent me an exploit

> for this 'virus'. It's a bit of C code that passes a UDP datagram packet
> with a few choice items in it, the most important being the word 'DOM' as
> one part, and a number (1 = reply, 2 = execute command). If you told the
> program (senrst) to send a command, it tries to add an entry to the
> infected host's inetd.conf file that listens on port 24554 that spawns an
> interactive shell. It then attempts to hup inetd. If you tell it to
> 'ping' the host, it tries to elicit a reply from the host. I got my
> infected host to reply only once, and the program (when in 'logging' mode)
> tends to be a bit trigger-happy-- a known non0-infected host is said to be
> infected.
>
> So, in my workings, I found that I couldn't get the arbitrary command to
> work. Even manually putting the inetd line and Hupping inetd myself
> didn't do anything! I was disappointed. I was hoping to play more.
>
> So, instead, I did some more analysis of what it does. It pretty much
> infects other binaries as you go along. I'm pretty sure that as you move
> around, it 'follows' you. For example, I went to /usr/bin and ran strings
> on a file-- and the hard drive thrashed for about 15 seconds before it
> gave me my output (and the file was very small). Once I ran strings the
> first time in that directory, it was fast, and of course, they all that
> the telltale sign of the infection.
>
> Infecting every single binary is an effective way for the virus to make
> sure the port is 'open': If I would find which pid was causing the port
> to open, and killed it, the port would stay close until I ran an infected
> binary (which is why you find such programs as ls, cd, and ssh as running
> on that port). If you did this:
> netstat -nap |grep 3049 |sed 's~/~ ~' |awk '{print \$6 }' |xargs kill -9
>
> It finds the pid, and kills it. Execute it two times in a row: and it
> hangs, because it's trying to kill it as it spawns it, or even before it
> exists. It's fun!
>
> REgardless, the 'virus' is pretty stupid. I'm leaving it on it's own
> separated network, and using another machine to watchi t's activity (no
> network activity whatsoever, besides 'who-has <hostname>'. It's not
> trying to spread to anything else, and it's not really taking info.
> Besides that, you have to be root for the virus to really take off, and
> when it does, it's really not useful. I was attempting to download a
> fixer, but the company wanted a lot of info, and wanted to scan my
> computer for proof before they gave it to me. Well, since I'm not about to
> port foreward to that box through my router, that's not likely.
>
> Anyway, I'd like to hear if anyone else has an exploit for it, otherwise,
> I'm going to try to adapt what I have to suit this 'virus'.
>
> Adam Bultman
>
> On Wed, 6 Mar 2002, Richard Hamnett wrote:
>

SecurityFocus Vuln-Dev: Re: Rumours about Apache 1.3.22 exploits -> analysis of so-called exploit client

> > *This is all very strange, i have a version of the exploit and i have run it*
> > *numerous times. It does not seem to affect any binaries nor does it open a*
> > *UDP backdoor port. I think the most likely explanation is what has been*
> > *mentioned previously, that it has been infected by someones machine*
> > *somewhere down the line*
> >
> > *please DO NOT waste your time and email me for the exploit, you know the*
> > *score.*
> >
> > *ill just give u as little info i can about the file i have*
> >
> > *-rwxr-xr-x 1 rick users 33189 Feb 27 17:26 73501867*
> >
> > *73501867: ELF 32-bit LSB executable, Intel 80386, version 1, dynamically*
> > *linked (uses shared libs), not stripped*
> >
> > *However i have set up a test rig with 'supposed' vulnerable versions of*
> > *apache and php*
> > *and i must add that the exploit did not work at all*
> > *but it didnt crash my apache like others have reported*
> >
> > *Regards*
> > *Richard Hamnett*
> >
> >
> > ----- Original Message -----
> > *From: "adamb" <adamb@twiki.iconideas.com>*
> > *To: <nilton.gs.sc@zipmail.com.br>*
> > *Cc: <vuln-dev@securityfocus.com>; <venom@phreaker.net>; <vugo@hotmail.com>*
> > *Sent: Wednesday, March 06, 2002 5:17 PM*
> > *Subject: Re: Rumours about Apache 1.3.22 exploits*
> >
> >
> > > *I have a copy of the virus; and I set up a test system last night. I made*
> > > *a clean install of slack 8.0 (I have a nother slack 8 box for*
> > > *comparison).*
> > >
> > > *I ran the infected file, and sure enough, the same thing happened: Added*
> > > *about 8 k to the files in /bin/, if you killed the process running the*
> > > *port 3049 listen, it would crop up. going to /proc/<pidnumber>., (getting*
> > > *the pid from netstat -nap |grep 3049) and*
> > > *doing a cat cmdline would show the program that was spawning the port*
> > > *opening.*
> > >
> > > *However, the port wasn't really being listened on. Sending packets,*
> > > *trying to connect via telnet did nothing. Evidently, according to the web*
> > > *pages I've been sent to says it's supposed to grab web pages, but my*
> > > *trojaned box didn't send any outgoing data (well, except for who-has*
> > > *statements for it's own hostname). Another page said it waits for special*
> > > *packets with 'DOM' at a specific offset before firing.*
> > >
> > >

SecurityFocus Vuln-Dev: Re: Rumours about Apache 1.3.22 exploits -> analysis of so-called exploit client

>>> Anyway, mine's sitting around, and I'm wondering what it's going to do. I
>>> don't consider the virus all that problematic, since it's not reaching out
>>> onto my network, and it's not spreading itself beyond it's own hard disk.
>>> I'm considering finding out what triggers this 'trojan' and writing
>>> something to trigger it.
>>>
>>> I've got a few logfiles -- typescripts of my activity, filesize changes,
>>> etc, that shows that it does stuff-- and I'll make more showing it's not
>>> listening to what I have for it...
>>>
>>> adam
>>>
>>>
>>> On Tue, 5 Mar 2002 nilton.gs.sc@zipmail.com.br wrote:
>>>
>>>> I had the same problem with a test box that I have on my network.
>>>>
>>>> I think the exploit called 73501867 is a trojan. It seems to infect ELF
>>>> binaries.
>>>>
>>>> When turn on the system (slackware 8.0 with kernel 2.4.5) I executed
>>>> 'netstat
>>>> -an' and nothing was showed up. But, about 3 minutes later when I
>>>> executed
>>>> 'netstat -an' it shows up:
>>>> Proto Recv-Q Send-Q Local Address Foreign Address
>>>> State
>>>>
>>>> udp 0 0 0.0.0.0:3049 0.0.0.0:*
>>>>
>>>> Do checksum in your files.
>>>>
>>>> Regards,
>>>> Nilton Gomes
>>>>
>>>> -- Mensagem original --
>>>>
>>>>> Actally I was pasted on a so called exploit this afternoon which claims
>>>>> to
>>>>> exploit via post but was only pasted on a binary,
>>>>> how ever please watch out for this I beleave its a working exploit but
>>>>> it
>>>>> also seems to open up a udp port on 3049 and some how seems to cloning
>>>>> the
>>>>> last proc , when stracing the 3049 all it seems to do is sit there and
>>>>> recv(...) and does nothing when you type anything.
>>>>>
>>>>> binary is called 73501867 - x86/linux mod_php v4.0.2rc1-v4.0.5 by
>>>>> lorian.
>>>>>
>>>>>> Has any one seen this about before?? Is this a trojan , if not then why

SecurityFocus Vuln-Dev: Re: Rumours about Apache 1.3.22 exploits -> analysis of so-called exploit client

> > > > *does*
> > > > *>it open udp 3049 even after a reboot.*
> > > > *>i trace the proc opening that port kill it and it seems to clone some*
> > *how*
> > > > *>my*
> > > > *>last proc and then 2mins l8r opens the port again.*
> > > > >
> > > > *>Any ideas?*
> > > > >
> > > > >
> > > > >----- *Original Message* -----
> > > > *>From: "Olaf Kirch" <okir@caldera.de>*
> > > > *>To: "H D Moore" <hdm@digitaloffense.net>*
> > > > *>Cc: <fractalg@highspeedweb.net>; <vuln-dev@securityfocus.com>*
> > > > *>Sent: Wednesday, February 27, 2002 3:07 AM*
> > > > *>Subject: Re: Rumours about Apache 1.3.22 exploits*
> > > > >
> > > > >
> > > > > *> There is a bug in the php_split_mime function in PHP 3.x and 4.x.*
> > *There*
> > > > *>is a*
> > > > > *> working exploit floating around which provides a remote bindshell*
> > *for*
> > > > *>PHP*
> > > > > *> versions 4.0.1 to 4.0.6 with a handful of default offsets for*
> > *different*
> > > > > *> platforms.*
> > > > >
> > > > > *Blechch. This code is really icky. There's really an sprintf down*
> > *there*
> > > > > *in the code that looks bad (apart from a few other things that look*
> > *bad).*
> > > > > *But if I don't misread the patch, the sprintf is still there in*
> > *4.1.1.*
> > > > >
> > > > > *> Since the PHP developers committed another change to the affected*
> > > > > *> source file (rfc1687.c) about two days ago, speculation is that*
> > *there*
> > > > *>is*
> > > > *>yet*
> > > > > *> another remote exploit.*
> > > > >
> > > > > *Not in the public CVS (has been removed?)*
> > > > >
> > > > > *Olaf*
> > > > > *--*
> > > > > *Olaf Kirch | --- o --- Nous sommes du soleil we love when we*
> > > > *play*
> > > > > *<okir@monad.swb.de / / / \ sol.dhoop.naytheet.ah*
> > *kin.ir.samse.qurax*
> > > > > *<okir@caldera.de +----- Why*

