

Re: IIS 4.0 DOS attack?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2001-07/0054.html>

From: Douglas R. Wilson (dallendoug@dallenhome.org)

Date: 07/20/01

From: "Douglas R. Wilson" <dallendoug@dallenhome.org>
Subject: Re: IIS 4.0 DOS attack?
To: focus-ms@SECURITYFOCUS.COM
Date: Thu, 19 Jul 2001 20:25:00 -0400
Message-ID: <web-11157738@capu.net>

Thank you to everyone who responded ---

here is my quick summary for the day, of things that may be useful to others . . .

I had 1 2k box that was supposedly patched --- culprit --- error in the patch distribution script we use (exploded hotfixes applied through batch files --- hotfix was in there, but didn't actually get applied when the script ran). Fix --- figure out that the script wasn't firing right, apply the patch, reboot. No more problems there.

Other box of note --- NT 4.0 SP6a IIS4 --- this one much more of a bear. with the symptoms of iis associated stuff getting knocked out every minute or so --- followed procedures, reinstalled patches, service pack, what have you --- nothing --- rinse, repeat, ad nauseum --- until someone pointed out that things weren't taking on some NT boxes. Went into IIS master properties, unmapped .idq and .ida (I owe thanks to whoever mailed me that tip --- feel free to step up and take credit), repatched and restarted, and voila! no more DoS . . .

A side note <rant> . . . A lot of people offered a lot of help --- but some people basically said "hey, dumbass, keep up on patches!" --- this is something that I try very hard to do, and am a big proponent of, but most organizations that are not very large in scope, or deep in pockets, may not be able to direct the resources needed to security, and so we make do with what we can, which may not be tested 3 times before it hits the field. As it turns out, a lot of our servers were fine --- we just had a few that fell through the cracks. But there is also a big difference between knowing that the eEye guys found this "code red" exploit a day or so ago (thank you very much for all the work you have done on that, BTW), and knowing what its symptoms will be in the real world, especially when you have to traverse the minefield of variables presented by a workplace that has clients, bosses, developers, admins, and techs all working together, or trying to at least.</rant>

SecurityFocus Microsoft: Re: IIS 4.0 DOS attack?

thanks again to everyone who responded.

doug

--

Douglas R. Wilson

dallendoug@dallenhome.org

On Thu, 19 Jul 2001 13:42:41 -0400 "Douglas R. Wilson" <dallendoug@dallenhome.org> wrote: > running into a frustrating situation, and wondering if anyone has > seen > anything like this before -- > > we have 2 servers on our network that keep having their w3svc crash > out > every few minutes, like clockwork. just started a few hours ago. No > strange updates/patches/etc made in the past day or so, servers have > been running for a while -- access to lots of clients and developers > though. > > We have several admins working on this -- sifting through logs, etc. > So > far, no real anomalies in HTTP logs (no requests with large or weird > packets -- but one server has so many logs, haven't been able to go > through all of them yet) -- but a lot of bogus FTP attempts detected > right before this started happening (ie logins from same IP w/ bogus > login/pass on both servers). This could be total coincidence, or > pre-strike probe. > > I know this is not a lot of info -- we are still gathering and > monitoring -- just wondering if this rang a bell with anyone. > > TIA, > > doug > > > -- > > Douglas R. Wilson > > dallendoug@dallenhome.org

- **Previous message:** [centipede: "Using hashes, not text credentials...?"](#)
- **In reply to:** [Douglas R. Wilson: "IIS 4.0 DOS attack?"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)