

# [Full-Disclosure] Re: OT: Akamai DNS and Yahoo

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-11/0345.html>

---

**From:** n3td3v (*xploitable\_at\_gmail.com*)

**Date:** 11/10/04

To: john.neiberger@efirstbank.com, security@yahoo-inc.com, full-disclosure@lists.netsys.com

Date: Tue, 9 Nov 2004 23:03:20 +0000

On Tue, 9 Nov 2004 23:02:15 +0000, n3td3v <xploitable@gmail.com> wrote:

> *On Tue, 09 Nov 2004 15:17:32 -0700, John Neiberger*

>

>

> *<john.neiberger@efirstbank.com> wrote:*

>>

>> *I saw many references about this in the archives but I haven't seen a*

>> *solution to it and we just started seeing this problem. Beginning*

>> *sometime very recently, our DNS servers are not able to resolve*

>> *www.yahoo.com. I have no problem if I point my PC to an external DNS*

>> *server, but when I point it back at our internal servers I get timeouts*

>> *when trying to resolve that domain.*

>>

>> *A Google search turned up dozens of posts over the past few years*

>> *regarding people not being able to resolve www.yahoo.com, but the*

>> *solutions don't seem to apply to our environment. We're running a*

>> *version of BIND 8 on Solaris 9, and it's likely that this behavior began*

>> *this weekend after we applied the most recent patch cluster for Solaris*

>> *9 and rebooted the server. For quite a while, all external DNS was*

>> *failing and we still have some odd intermittent problems but the most*

>> *noticeable issue that is 100% reproducible is the failure to resolve*

>> *Yahoo addresses.*

>>

>> *I saw a few Usenet posts that mentioned this could be a problem with*

>> *Extensions for DNS and the fact that DNS replies could be larger than*

>> *512 bytes. This would be a problem if you were behind a PIX firewall*

>> *running a certain version of software and with a certain feature*

>> *configured because it would drop all UDP DNS packets over 512 bytes.*

>> *This doesn't really fit our environment so I'm still looking for*

>> *answers.*

>>

>> *Any thoughts?*

>>

>> *Thanks,*

>> *John*

>> --

>

Full-Disclosure: [Full-Disclosure] Re: OT: Akamai DNS and Yahoo

- > Yes, yahoo had an incident with its DNS in the past week(s) with its
- > dns configuration with regards of "akadns". Yahoo! security team were
- > alerted my myself as soon as abnormal behaviour was reported by the
- > scripts i have running on various yahoo and aka servers to get upto
- > date status.
- >
- > The problem first started from what I monitored from Yahoo! having the
- > address in the address bar as "yahoo.akadns.com" to Yahoo! serving a
- > blank HTML/PHP as the homepage, while still showing "Yahoo!" as the
- > HTML title of the homepage document. (proving my network was not at
- > fault from network disruption, yahoo and more focused akadns was to
- > blame for the spate of outages one day in the past week(s).)
- >
- > I'll talk to you further in private if you wish, or on the list
- >
- > ....
- >
- > Thanks, n3td3v
- >
- > <http://www.geocities.com/n3td3v>
- >
- > I'm a security enthusiast
- >

---

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>