Aplura, LLC
5653 Blithaire Garth
Columbia, MD 21045
301-523-2110 (w)
410-864-8386 (f)

Focused Information Security
www.aplura.com

DNS Cache Pollution Vulnerability

Overview

Secret meetings to fix DNS, a massive world-wide patch-release effort, warnings from security experts, yet many DNS systems are still un-patched weeks after exploits entered the *wild*.

The DNS Cache Pollution vulnerability, *IS* a big deal, and all clients and servers should be patched immediately, even if they are not on the public Internet.

Any host on your network that is under attacker-control (bot, spyware, or some other malware) has the potential to spoil the cache of your resolver. This makes every system a potential attack-vector to an un-patched/unprotected resolver. All windows Active Directory systems, and all dedicated DNS servers are the most critical.

Read below why Microsoft did not classify this bug as **critical** even though the rest of the world is treating it as such.

Vulnerability Background

A critical flaw was discovered in the Internet's Domain Name Service (DNS) that effects every Internet user. In short, with this new discovery, it is trivial for an attacker to poison the cache of a DNS resolver, effectively redirecting traffic destined for a legitimate domain to a server managed by the attacker.

Any type of Internet traffic that uses DNS is vulnerable including: web, mail, ftp, IM, and file sharing.

Security hacking tools are available which which automate the attack, allowing an attacker to compromise a target resolver in under 10 seconds.

An example of the threat is this: The attacker poisons the resolver cache of company *FooCom* for the records which point to a FooCom Intranet site, business partner, or any other site such as www.yahoo.com. After the attack, any user at *FooCom* when browsing to a domain that was compromised by the attacker, could be instead redirected to the attacker's own version of the site. To the user, nothing is amiss, as the browser will provide no warning. Additionally, the attacker than can proxy all of these sessions back to the real site, allowing the user to login and conduct business, meanwhile the attacker gathers all of the session data including user credentials, urls, and any other data sent between the user and the server.

The attack works just as well with e-mail. If the attacker poisons the DNS cache all, e-mail for a compromised domain will be redirected to the mailserver controlled by the attacker. The attacker can then make a copy of each message and then bounce the message to the legitimate recipient. The message arrives so the sender and recipient are not suspicious, but the attacker now has a copy of every message sent to that domain.

Vulnerability Test

Are you vulnerable to the DNS Cache Pollution problem? If the DNS resolvers that you use to browse the Internet or send e-mail (the resolvers your mailserver uses) has not been patched then you ARE vulnerable. Want to test it from your desk? Follow the instructions below.

Due to the nature of the bug, one can determine vulnerability-status by analyzing the packets in their outbound resolution request. If this sounds complicated, don't worry, a number of sites have popped up that will do this for you and then issue a conditioned response based on your query. All you need to do is an nslookup against a specific address and look at the response.

- In Windows

1. Open a command window
    - If you are using anything other than Vista do (start | run | type 'cmd' |return)
2. In the command window type this:
    - `nslookup -type=txt -timeout=30 porttest.dns-oarc.net`

- In Linux/Unix

1. Open a command shell
2. In the command window type this:
    - `dig +short porttest.dns-oarc.net TXT`

If you get a response that says **BAD** or **POOR**, then you might want to consider changing the resolver you use to one that is patched. Otherwise, it should say **GOOD** or **GREAT**

Read more about testing your connection on the dns-oarc site.

Countermeasures

There are a number of countermeasures for this attack, though patching is the best method. The world's DNS software providers orchestrated an industry-wide effort to release patches quickly. Patches are available for all major and most minor distributions. If this is not possible immediately, consider alternatives until it is possible.

One alternative is to use a different recursive DNS provider such as OpenDNS. OpenDNS is a group who runs safe-open cache resolvers at no charge. They say it is safe. Generally-speaking it probably is, but take this with a *grain of salt*.

There are also steps you can take within your configuration such as restrict what clients can perform DNS resolution against your resolver, or to implement DNSSEC within your environment.

Patch Impact

Here is brief analogy posted by Dan Kaminskyon his blog on July 26th, 2008

Different analogy:

- Before the attack: A bad guy has a one in sixty five thousand chance of stealing your Internet connection, but he can only try once every couple of hours.
- After the attack: A bad guy has a one in sixty five thousand chance of stealing your Internet connection, and he can try a couple thousand times a second.
- After the patch: A bad guy has a one in a couple hundred million, or even a couple billion chance of stealing your Internet connection. He can still try to do so a couple thousand times a second, but it’s going to make a lot of noise.

Windows Patches

Microsoft has released Microsoft Security Bulletin MS08-037 and the following corresponding patches:

- KB951746 - Server-Side
- KB951748 - Client-Side

The patches have been available for weeks, and even after the *August 5th,* Microsoft *Patch* Tuesday, many systems remain vulnerable. Why?

Microsoft did not classify the patches as critical, and therefore they do not get installed by default through the normal update process.

One question that everyone continues to ask is, *If this is such a big problem, why are these not listed as critical?*

It made sense that Microsoft had some classification criteria, and that maybe the checkboxes at the end of the evaluation did not add-up to **Critical**, but why?

Thanks to an analyst friend, he had an answer: The DNS vuln requires a higher level of technical ability and an attacker (or tool) to directly interact with and exploit a vulnerable system. In short, the vuln isn't a critical because it can't (as far as anyone knows) act as a propagation mechanism for a worm. Here is Microsoft's rating criteria

Vulnerability Timeline

- 200803xx - Dan Kaminsky (famous security researcher) while looking into another issue, discovered a big problem with DNS and how it structures queries.
  - He coordinated with the largest DNS implementation vendors, and initially reported to CVE via CVE-2008-1447
  - The research and response effort was done in secret.
- 20080708 - Still a mystery, the DNS problem is reported to US-CERT and others, concerns rise.
- 20080709 - Dan Kaminsky details his efforts over the last six months. Dan continues to keep a lid on the actual problem.
- 20080717 - Dan Kaminsky notes on his blog that he will release the info regarding the DNS problem at Blackhat on *August 6th*.
- 20080721 - A security practitioner who worked on the DNS response effort publicized the details of the bug by posting an unauthorized entry to his personal blog. It was quickly discovered and removed, but with world-wide-syndication of the blog, it was too late. The bug **details were out**!
  - Dan Kaminsky noted on his blog that he bought the world 13 Days to patch which is the time between when the bug was announced and when the details were revealed.
- 20080722 - With the details revealed, patching for this vulnerability should now be EVERY DNS administrator's top priority.
- 20080724 - Exploits are available in the wild, specifically Metasploit now has a module to automate the attack against a vulnerable resolver.
  - Dan Kaminsky post his own details of the bug.
- 20080730 - Exploits reported in the wild on ISP networks.

Resources

- Test for the bug - https://www.dns-oarc.net/oarc/services/porttest
- Dan Kaminsky (researcher who discovered the bug) - http://www.doxpara.com/
- Microsoft Security Bulletin MS08-037 http://www.microsoft.com/technet/security/bulletin/ms08-037.mspx
- CVE-2008-1447 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447