Responsible Disclosure

A Case Study of CERT VU#800133, “DNS Cache Poisoning Issue”

Sid Faber, sfaber@cert.org
2008 OARC Workshop
September 24, 2008
Agenda

- Discovery
- Patch
- Disclosure
- Exploit
- Conclusions
Acknowledgements

This work would not have been possible without assistance from:

- The Security Information Exchange, https://sie.isc.org (data)
- Paul Vixie (coordination, validation)
- Duane Wessels (computing resources)
- Chad Dougherty (CERT Vulnerability Analysis)
- Nick Ianelli (CERT Malicious Code)
Discovery

(ssshhhhh....)
Timeline

Kaminsky Discovery
  • February 2008 (?)

Notification to a small number of interested parties
  • 2008.03.19

DNS Summit, 2008.03.31
  • Detailed disclosure
  • Proposed solution
  • Proposed patch date 2008.08.07
  • Detailed release date at Blackhat
What is this?

DNS cache poisoning is not a new concept

- Query ID (QID, aka TXID) is only a 16-bit number
- UDP spoofing

Not so much a vulnerability as a new technique:

- Additional resource records (RRs) in the spoofed responses get cached
- Avoid the timeout wait by asking random questions
- Payload is in Additional RRs rather than Answers
What’s the (interim) fix?

Increase entropy with a random ephemeral port

- Traditionally most name servers grab a random port at startup and hang on to it for all future queries

Before: guess TrxID: one in 65,536 ($2^{16}$)

After: guess TrxID ($2^{16}$) and ephemeral port ($\sim2^{14}$)
Timeline

- **March 19**, CERT initial contact
- **March 31**, DNS Summit at Microsoft
- **July 8**, Proposed Patch Date
- **Blackhat, August 7**
- **Kaminsky discovers flaw at Blackhat, August 7**
Vulnerability coordination/response

After DNS summit, CERT begins notifying vendors

- First round: survey message, no details seeking independent DNS implementers
- Second round: detailed technical message and timeline

Roughly 150 vendors contacted

- Vendor communication is performed securely using PGP and our custom internal contact management application

2008.07.08: Announcement and patches released
Patch

…and patch, and patch, and patch…
Timeline

March
- Kaminsky discovers flaw
- 3/19, CERT initial contact
- 3/31, DNS Summit at Microsoft

April
- CERT VU #800113, 7/8

May

June

July
- Patch Rollout
- Blackhat, 8/7

August
Review: Basic DNS Architecture

1. Caching Client
2. Caching Resolver
3. Authoritative Server
4. Caching Client

www.acme.com = 10.1.2.3

Vulnerable Vulnerable
### Review: Flow Collection

![Diagram showing network flow](image)

<table>
<thead>
<tr>
<th></th>
<th>sIP</th>
<th>dIP</th>
<th>sPort</th>
<th>dPort</th>
<th>proto</th>
<th>pkt</th>
<th>byte</th>
<th>sTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.254.105.86</td>
<td>186.54.105.135</td>
<td>1027</td>
<td>53</td>
<td>17</td>
<td>1</td>
<td>282</td>
<td>2008/06/11T12:00:02</td>
</tr>
<tr>
<td>2</td>
<td>186.54.105.135</td>
<td>17.131.109.185</td>
<td>34574</td>
<td>53</td>
<td>17</td>
<td>1</td>
<td>306</td>
<td>2008/06/11T12:00:02</td>
</tr>
<tr>
<td>3</td>
<td>17.131.109.185</td>
<td>186.54.105.135</td>
<td>53</td>
<td>34574</td>
<td>17</td>
<td>1</td>
<td>554</td>
<td>2008/06/11T12:00:03</td>
</tr>
<tr>
<td>4</td>
<td>186.54.105.135</td>
<td>10.254.105.86</td>
<td>53</td>
<td>1027</td>
<td>17</td>
<td>1</td>
<td>403</td>
<td>2008/06/11T12:00:03</td>
</tr>
</tbody>
</table>
Identifying Unpatched Workstations

ISP’s Server or Open Recursive Resolver

Instrumentation

<table>
<thead>
<tr>
<th>sIP</th>
<th>dIP</th>
<th>sPort</th>
<th>dPort</th>
<th>pro</th>
<th>pkt</th>
<th>byte</th>
<th>sTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.254.105.86</td>
<td>186.54.105.135</td>
<td>1027</td>
<td>53</td>
<td>17</td>
<td>1</td>
<td>282</td>
<td>2008/06/11T12:00:02</td>
</tr>
<tr>
<td>10.254.105.86</td>
<td>186.54.105.135</td>
<td>1031</td>
<td>53</td>
<td>17</td>
<td>1</td>
<td>282</td>
<td>2008/06/11T12:00:21</td>
</tr>
<tr>
<td>10.254.105.86</td>
<td>186.54.105.135</td>
<td>1032</td>
<td>53</td>
<td>17</td>
<td>1</td>
<td>282</td>
<td>2008/06/11T12:00:21</td>
</tr>
<tr>
<td>10.254.105.86</td>
<td>186.54.105.135</td>
<td>1058</td>
<td>53</td>
<td>17</td>
<td>1</td>
<td>282</td>
<td>2008/06/11T12:01:03</td>
</tr>
</tbody>
</table>
Home User Results

Graph showing the percentage of unique hosts per hour with different colors indicating Random, Static, and Guessable categories. The x-axis represents dates from 07/12 to 08/09.
Results Explained

Green: Ephemeral port is unpredictable
Red: Ephemeral port is static
Blue: Ephemeral port is predictable (25% chance)
Yellow: Host Count
Home User Timeline

- 70% vulnerable at T0
- 47% vulnerable after first weekend
- Almost no predictable hosts

- Not much improvement in 2\textsuperscript{nd} week
- Complete after one month

7/12 7/19 7/26 8/02 8/09

Percentage

Unique Hosts per Hour
Timeline revisited

- **Home User Patching Complete, 8/4**
- **Home User Bounce, 7/11**
- Kaminsky discovers flaw
- **3/19, CERT initial contact**
- **3/31, DNS Summit at Microsoft**
- **CERT VU #800113, 7/8**
- **Blackhat, 8/7**
Identifying unpatched servers

For an unpatched resolver, each connection uses the same ephemeral port.

Patched resolvers use a random ephemeral port.

Instrumentation

<table>
<thead>
<tr>
<th>sIP</th>
<th>dIP</th>
<th>sPort</th>
<th>dPort</th>
<th>pro</th>
<th>pkt</th>
<th>byte</th>
<th>sTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>186.54.105.135</td>
<td>16.64.195.188</td>
<td>32556</td>
<td>53</td>
<td>17</td>
<td>1</td>
<td>282</td>
<td>2008/06/11T12:00:02</td>
</tr>
<tr>
<td>186.54.105.135</td>
<td>203.37.75.8</td>
<td>32557</td>
<td>53</td>
<td>17</td>
<td>1</td>
<td>258</td>
<td>2008/06/11T12:00:21</td>
</tr>
<tr>
<td>186.54.105.135</td>
<td>114.154.44.64</td>
<td>32558</td>
<td>53</td>
<td>17</td>
<td>1</td>
<td>322</td>
<td>2008/06/11T12:00:21</td>
</tr>
<tr>
<td>186.54.105.135</td>
<td>21.87.225.250</td>
<td>32559</td>
<td>53</td>
<td>17</td>
<td>1</td>
<td>196</td>
<td>2008/06/11T12:01:03</td>
</tr>
</tbody>
</table>
Enclave Server Results

![Graph showing Enclave Server Results](image)
Enclave Server Results (2)

62% vulnerable at T0

First week ~10% improvement

Steady 8% per week improvement

Complete after one month; 25% still vulnerable

Higher percentage of predictable hosts
Timeline--including patching

Patching Complete after 4 weeks
10% - 25% First Week Bounce

Kaminsky discovers flaw
3/19, CERT initial contact
3/31, DNS Summit at Microsoft

CERT VU #800113, 7/8

Blackhat, 8/7
Disclosure

What was that again? Oh, of course…
Reaction to initial release

Posted in an Underground IRC channel (which was talking about marijuana):

- Reaction: "haha nice"
Is your server vulnerable?

Community tools to test if your server was vulnerable:

- 2008.07.11 (OARC) dig +short porttest.dns-oarc.net TXT
- 2008.07.14:
  - http://www.doxpara.com

3/19, CERT initial contact
3/31, DNS Summit at Microsoft
CERT VU #800113, 7/8
Blackhat, 8/7
Details disclosed…no…wait…well…umm…

- **2008.07.21**: IRC bot pushes the following URL:
  - [Slashdot] Kaminsky's DNS Attack Disclosed, Then Pulled (it)
    - http://it.slashdot.org/article.pl?sid=08/07/21/2212227

- **2008.07.22**: The following link is posted in various underground IRC channels:

Diagram:
- 3/19, CERT initial contact
- 3/31, DNS Summit at Microsoft
- CERT VU #800113, 7/8
- Blackhat, 8/7
Information in the underground (2)

• **2008.07.22**: In the middle of a discussion the following two items were posted:
  - "It seems the cat might be out of the bag regarding Dan Kaminsky's upcoming presentation at Blackhat."

• Link also posted in various underground IRC channels

---

3/19, CERT initial contact
3/31, DNS Summit at Microsoft
CERT VU #800113, 7/8
Blackhat, 8/7
Timeline--including disclosure

- Kaminsky discovers flaw
  - 3/19, CERT initial contact
  - 3/31, DNS Summit at Microsoft
- CERT VU #800113, 7/8
- Testing Tools Available, 7/11
- Flaw details released, 7/21
- Blackhat, 8/7

Patching Complete after 4 weeks
10% - 20% First Week Bounce
Exploit

*mwa ha ha ha ha*¹

¹An interjection. Used to denote evilness.


<http://www.urbandictionary.com/define.php?term=mwa%20ha%20ha%20ha%20ha%20ha>
Publicly available exploits

- **2008.07.23**: Metasploit
  - Two days after details released
  - Part of the Metasploit framework
  - Posted on various Underground IRC channels on 2008.07.27 and 2008.08.09

3/19, CERT initial contact
3/31, DNS Summit at Microsoft

CERT VU #800113, 7/8
Flaw details released, 7/21
Blackhat, 8/7
Publicly available exploits (2)

- **2008.07.24**: Metasploit v2
  - Primary difference: NS injection
  - Part of the Metasploit framework

---

3/19, CERT initial contact
3/31, DNS Summit at Microsoft

- CERT VU #800113, 7/8
- Flaw details released, 7/21
- Blackhat, 8/7
Publicly available exploits (3)

- **2008.07.24**: milw0rm
  - [http://www.milw0rm.com/exploits/6130](http://www.milw0rm.com/exploits/6130)
  - C based exploit

- 3/19, CERT initial contact
- 3/31, DNS Summit at Microsoft
- CERT VU #800113, 7/8
  - Flaw details released, 7/21
  - Blackhat, 8/7
Publicly available exploits (4)

- **2008.07.28**: Evilgrade
  - Evilgrade framework includes DNS cache poisoning
  - URL picked up on some underground IRC Channels:
    

3/19, CERT initial contact
3/31, DNS Summit at Microsoft
CERT VU #800113, 7/8
Flaw details released, 7/21
Blackhat, 8/7
Publicly available exploits (5)

- **2008.08.04**: adns
  - Asynchronous-capable DNS client library and utilities
  - Two weeks following detailed disclosure
  - Minor DNS utility, yet enough of a following to generate an exploit

**Timeline:**
- 3/19, CERT initial contact
- 3/31, DNS Summit at Microsoft
- CERT VU #800113, 7/8
- Flaw details released, 7/21
- Blackhat, 8/7
We have attacks!

- **2008.07.30**
  - Confirmation obtained that sites are compromised via DNS Cache poisoning attacks
  - A full week after exploits were available

- **2008.08.21**
  - DNS cache flaw used to poison Chinese ISP's server
Timeline Yet Again

- **Patch Rollout**
- **March**
  - Kaminsky discovers flaw
  - 3/19, CERT initial contact
  - 3/31, DNS Summit at Microsoft

- **April**
  - CERT VU #800113, 7/8
  - Testing Tools Available, 7/11
  - Flaw details released, 7/21
  - POC & Framework Exploits Available, 7/23
  - Attacks Begin, 7/30

- **May**
  - 10% - 20% First Week Bounce

- **June**
  - Patching Complete after 4 weeks

- **July**
  - Blackhat, 8/7
Conclusions

Gee, I think I already knew that…
Perhaps two timelines?

**Patch Release**

- Discovery
- Coordination
- Limited Vendor Disclosure
- Patching Complete
- Full Public Disclosure
- Exploits Available
- Attacks Begin

4 wks
14 weeks
4 wks
14 days
2d
7 days
Specific Observations

Timeline

- Extended time between private disclosure and patch only added minimal risk
- Proposed 30-day window between patch and disclosure was sufficient
- Early disclosure caused attacks before patch rollout had been completed

Who has patched?

- 20-25% remained vulnerable
- 5-10% impacted by “gateway” issue
General Conclusions

Responsible Disclosure Worked

- Despite publicity, only 10-20% of machines patched within a week
- Within a month, most patches had been applied
- Critical milestone / warning sign for risk management is detailed disclosure
- There’s still some time between disclosure and attack.

There’s nothing really new here, just a quantitative confirmation of past qualitative observations.
Responsible Disclosure

A Case Study of CERT VU#800133, “DNS Cache Poisoning Issue”

Sid Faber, sfaber@cert.org
2008 OARC Workshop
September 24, 2008
For More Information

Visit the CERT® web site
http://www.cert.org/

Contact Presenter
Sid Faber, sfaber@cert.org

Contact CERT
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890

Hotline:
412-268-7090
CERT/CC personnel answer 8:00 a.m.–5:00 p.m.
and are on call for emergencies during other hours.

Fax:
412-268-6989

E-mail:
cert@cert.org