CERT VU#800113

Multiple DNS implementations vulnerable to cache poisoning

Alan Clegg

Support Engineer

Keith Mitchell

Director of Engineering

Internet Systems Consortium

alan_clegg@isc.org

keith_mitchell@isc.org

Version 1.3

Cache Poisoning

- The ability to introduce incorrect information into a DNS server's cache
- This information is then provided to clients

CERT VU#800113

- Multiple DNS implementations are extremely vulnerable to cache poisoning
- Vulnerable
  - BIND, Cisco, Juniper, Microsoft and derivatives
- Not immediately vulnerable
  - djbdns, powerDNS, unbound

CERT VU#800113

- Dan Kaminsky discovered a new vector for an attack against DNS transactions

- Issue (small size of transaction ID) known for years, but Dan's attack vector is “more impressive”

CERT VU#800113

- Dan contacted several vendors upon discovery of the vulnerability
- Those vendors worked together to release information on the same day
- Yes, it was a Patch Tuesday

CERT VU#800113

- ISC, Cisco, Microsoft, Debian and others (but not everyone) were alerted and released code simultaneously

- This was a major effort

  (that is a major understatement)

CERT VU#800113

- The exploit is real
- Additional details were released to the public at Black Hat on August 7th
- The Internet has changed

CERT VU#800113

- Flaw is “FedEx Logo Arrow” type of vulnerability

- Once you see it, you won't be able to “not see it”

CERT VU#800113

- The only long-term fix is DNSSEC
- The temporary work-around is to add randomness to each query
- Randomness is introduced in the query port number

CERT VU#800113

- Note that even "not immediately" vulnerable servers listed earlier are still theoretically vulnerable

- The current "fix" of port randomization is remediation until DNSSEC is deployed

CERT VU#800113

- Deploying DNSSEC is not realistic in the short term
- Port randomization of queries adds randomness, but is a temporary fix
- Update & Configure ASAP
- Other interim fixes being considered by IETF DNSEXT WG:
  - e.g. “DNS 0x20”

CERT VU#800113

- BIND
  - Install 9.3.5-P2, 9.4.2-P2, 9.5.0-P2
    - Note that initial -P1 releases **are** secure, but had some performance and stability issues on some platforms (e.g. Solaris) which -P2 release mitigate
    - -P1 fine if you are not seeing problems
    - -P2W releases very shortly now to address some Windows-specific issues
  - Remove restrictions on query ports

```
query-source address 192.168.2.3 port 53;
```

Are you vulnerable?

- Dan Kaminsky
  - Web based interface - `www.doxpara.com`

```
Your name server, at 66.57.17.110, appears to be safe.
Requests seen for fbdfd8f7dc64.toorrr.com:
66.57.17.110:57889 TXID=65162
66.57.17.110:60521 TXID=53424
66.57.17.110:21698 TXID=32752
66.57.17.110:24178 TXID=49020
66.57.17.110:47197 TXID=25844
```

Are you vulnerable?

- Michael C. Toren
  <mct@toren.net>

- Perl based reverse engineering of Dan's javascript

  http://michael.toren.net/code/noclicky/

Are you vulnerable?

- Duane Wessels
  <wessels@dns-oarc.net>

```
dig +short porttest.dns-oarc.net TXT

"66.57.17.110 is GOOD: 26 queries in 2.6
  seconds from 26 ports with std dev
  19167.29"
```

Are you vulnerable?

- Duane Wessels
  <wessels@dns-oarc.net>

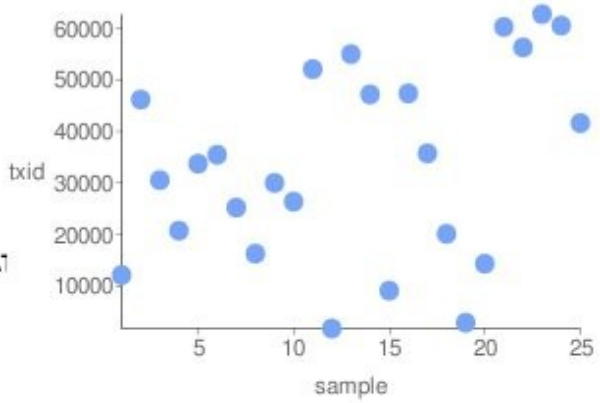
https://www.dns-oarc.net/oarc/services/dnsentropy

By far our favorite!

(even if it is web based)

Are you vulnerable?

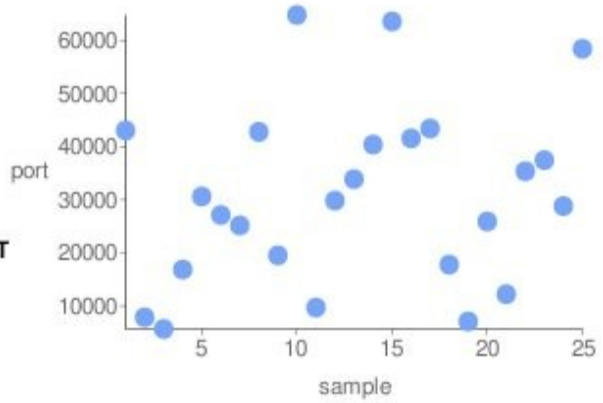
66.57.17.110 Transaction ID Randomness: GREAT



Number of samples: 25
Unique txids: 25
Range: 1747 - 62732
Modified Standard Deviation: 18690
Bits of Randomness: 16
Values Seen: 12097 46163 30527 20723 33718 35451 25210 16277 29988 26355 52063 1747 54978 47159 9086 47348 35725 20113 2878 14319 60249 56271 62732 60512 41599

Are you vulnerable?

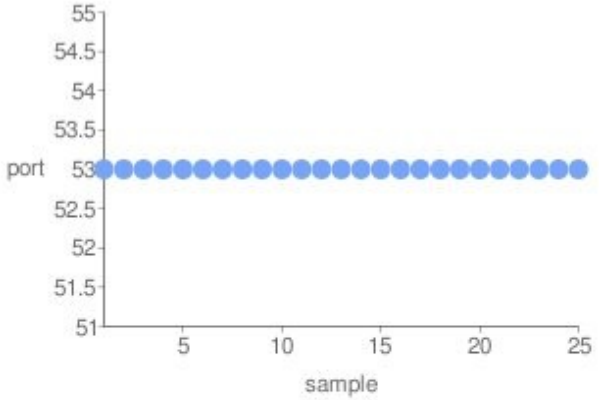
66.57.17.110 Source Port Randomness: GREAT



Number of samples: 25
Unique ports: 25
Range: 5691 - 64785
Modified Standard Deviation: 16827
Bits of Randomness: 16
Values Seen: 43054 7891 5691 16897 30628 27141 25182 42783 19549 64785 9724 29847 33894 40400 63576 41563 43425 17799 7114 25924 12237 35382 37464 28826 58425

Are you vulnerable?

Source Port Randomness: POOR



Number of samples: 25
Unique ports: 1
Range: 53 - 53
Modified Standard Deviation: 0
Bits of Randomness: 0
Values Seen: 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53

DNSSEC vs port randomization

- there is excellent cause for fear, and no reason to expect that udp port randomization is going to last forever in the face of new threats, both some i've considered or heard of, and others we can only dream of. DNS is too attractive a target, too much fruit hanging too low for too long, to imagine that we'll be crypto-free for our lifetimes.

Paul Vixie

July 10, 2008

DNS-Operations ML

Kaminsky's Thoughts

- There are four possibilities [regarding how you view the criticality of the alert]:

  1. DNS doesn't matter. Don't patch.
  2. It's bad, but old. Don't patch.
  3. It's bad, but old. Patch.
  4. It's bad, and new. Patch.

- I [Kaminsky] argue #4. I don't care about #3 -- the less time people spend trying to find what's new, the better. I'm terrified about #1 and #2.