CERT VU#800113

Multiple DNS implementations vulnerable to cache poisoning

Alan Clegg

Support Engineer

Internet Systems Consortium

alan_clegg@isc.org

Version 1.0

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 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 will be released to the public at Black Hat on August 7th
- At that point, the Internet will change

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

- Unlike many vulnerabilities, the patch does not point directly to the vulnerability

- There is always the chance of “early discovery”

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

CERT VU#800113

- BIND
  - Install 9.3.5-P1, 9.4.2-P1, 9.5.0-P1
  - 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"
```

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.