

BIND 8 EOL and BIND 8 DNS Cache Poisoning (Amit Klein, Trusteer)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-08/msg00432.html>

- *From:* "Amit Klein" <aksecurity@xxxxxxxxx>
 - *Date:* Mon, 27 Aug 2007 21:01:56 +0200
-

BIND 8 EOL and BIND 8 DNS Cache Poisoning

Note: this is a different attack from BIND 9 DNS cache poisoning.

I discovered a new weakness in BIND 8 DNS server which enables "DNS Forgery Pharming". An attacker can remotely poison the cache of any BIND 8 caching DNS server and force users who use this DNS server to reach fraudulent websites each time they try to access real websites. BIND 8 is still a very popular DNS server nowadays thus this attack applies to a big part of Internet users.

The concept of DNS cache poisoning was discussed many times before. However, this attack was considered impractical for the leading industrial DNS servers due to the transaction ID mechanism that DNS servers implement today. The transaction ID is supposed to be a secure, random number that the attacker must guess in order to poison the DNS cache. There are 65,536 combinations which make enumeration impractical in the current network conditions.

I've recently found a weakness in the transaction ID generation algorithm of BIND 8 (both for USE_POOL and for SHUFFLE_ONLY algorithm variants). By observing a few consecutive transaction IDs from the same DNS server an attacker can predict its next value. BIND 9's new algorithm is similar to BIND 8's USE_POOL algorithm (but somewhat stronger). For BIND 9, a theoretic attack was demonstrated (requires too many guesses at this stage, but possibly may be improved in the future).

This weakness can be turned into a mass attack in the following way:
(1) the attacker lures a single user that uses the target DNS server to click on a link. No further action other than clicking the link is required
(2) by clicking the link the user starts a chain reaction that eventually poisons the DNS server's cache (subject to some standard conditions) and associates fraudulent IP addresses with real website domains.
(3) All users that use this DNS server will now reach the fraudulent website each time they try to reach the real website.

The attack only works when the BIND server is relatively "fresh", i.e.

BIND 8 EOL and BIND 8 DNS Cache Poisoning (Amit Klein, Trusteer)

that it didn't process a lot of queries since it was started (see the paper for full details).

The algorithms for predicting the transaction ID were coded in Perl and were demonstrated to work well (and fast!).

The algorithms, as well as the paper, are available Trusteer's website:

Full paper: <http://www.trusteer.com/docs/bind8dns.html>

ISC were informed on July 26th,

ISC has now declared BIND 8 EOL and recommends upgrade to BIND 9.4.1-P1

Alternative Interim solution: Install patch "P1" for BIND 8.4.7

Versions are available on <http://www.isc.org/>

Thanks,
Amit Klein
CTO
Trusteer
www.trusteer.com