

Paper by Amit Klein (Trusteer): "PowerDNS Recursor DNS Cache Poisoning [pharming]"

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-04/msg00004.html>

- *From:* Amit Klein <amit.klein@xxxxxxxxxxxxx>
 - *Date:* Mon, 31 Mar 2008 15:07:19 +0300
-

Hello BugTraq

Once again, a DNS cache poisoning against a popular DNS cache server. This time, it's PowerDNS (the third most popular DNS server, servicing over 40 million users). The vendor coded several impressive security measures against DNS spoofing (e.g. UDP source port randomization and spoofed response detection), but relied on the standard C randomization facility (the `rand()` and `srand()` functions in `<stdlib.h>`). The two popular `stdlib` implementations analyzed, `glibc` (used with GNU C++ for Linux/Unix-like systems) and `MSVCRT` (used with Microsoft's `MSVC` for Windows) are shown to be easily predictable, thus enabling an attacker to predict the DNS queries sent by PowerDNS Recursor, and in turn mount an efficient and effective DNS cache poisoning attack (or a pharming attack, as it is often called today).

PowerDNS's security contact, Bert Hubert, responded in a quick and professional manner – an immediate fix was silently incorporated (with my blessing) in Recursor 3.1.5–snapshot5 which was released less than 6 hours after the initial report. A stable version, Recursor 3.1.5, that "officially" includes the fix, is announced today, and is available for immediate download (see <http://doc.powerdns.com/powerdns-advisory-2008-01.html>).

The full analysis can be found in the following link:

<http://www.trusteer.com/docs/powerdnsrecursor.html>

Thanks,
–Amit
CTO, Trusteer