

Wednesday, July 23, 2008

### DNS cache poisoning exploit released

Hi There,

There is a new DNS Cache poisoning disclosure that has been inadvertently leaked before it was scheduled to be released by Dan Kaminsky (IOActive). This is a very serious flaw in the DNS protocol that impacts caching resolvers, like the resolvers hosted at your service provider that help your workstation resolve IP addresses to domain names.

This bug does not directly impact authoritative name servers like the ones used to host your domain names at EasyDNS. Our name servers do not request answers from external sources, and rely entirely on internal cache files to offer answers. So for example, nobody will be able to change your IP information on our end. That part of the bug is unfortunately located at the caching end.

That being said; this is still a serious flaw, and we are taking this opportunity to upgrade the DNS software on our authoritative name servers to ensure that we are 100% compatible across the board with the newly upgraded caching name servers located at your Internet Service Provider. These upgrades should not impact name resolution if you are using more than one of our name servers to serve answers for your domain name (actually, please ensure that you are).

To make sure your Internet Service Provider is up to speed, you can use Dan Kaminsky's test script at DoxPora Research. If your Internet Service Provider is not yet up to speed, you may want to give them a nudge and/or change your DNS resolver configuration to a more trusted service. Update It is now making news that an exploit to this attack has been released., please see our post about our newly launched DNSresolvers.com if you are looking for safe resolvers.

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 20:52