

# After 6 months – fix available for Microsoft DNS cache poisoning attack

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-11/msg00174.html>

---

- *From:* Amit Klein <[amit.klein@xxxxxxxxxxxxx](mailto:amit.klein@xxxxxxxxxxxxx)>
  - *Date:* Tue, 13 Nov 2007 20:26:43 +0200
- 

After 6 months – fix available for Microsoft DNS cache poisoning attack

On April this year I discovered a new vulnerability that enables DNS cache poisoning attack against the Windows DNS server. Today (November 13th, 2007) – six and a half months after being informed – Microsoft released a fix for this vulnerability. As the fix is now publicly available, I can finally share my research finding with you.

For those of you who read my research papers on BIND 8 and 9 (<http://www.trusteer.com/docs/research.html>) – it is the same type of attack but a different vulnerability and a different DNS server. It's interesting that both BIND and Microsoft had different, and at the same time fundamentally flawed implementations of DNS (with Microsoft's implementation being more easily predictable than those of BIND).

Using this attack an attacker can remotely poison the cache of any Windows DNS server (when run in caching mode) and force users who use this DNS server to reach fraudulent websites each time they try to access real websites.

Windows DNS Server (part of Windows 2003 Server and Windows 2000 Server) is a popular DNS server (especially in Microsoft-based sites).

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 possible transaction ID values which make enumeration impractical in the current network conditions.

The weakness I found is in the transaction ID generation algorithm of Windows DNS Server. By observing a few consecutive

## After 6 months – fix available for Microsoft DNS cache poisoning attack

transaction IDs from the same DNS server an attacker can predict its next value.

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 algorithm for predicting the transaction ID is very simple. It was coded in Perl and was demonstrated to work well (and fast!).

The algorithm, as well as the paper, are available on Trusteer's website: <http://www.trusteer.com/docs/windowsdns.html>

Microsoft were informed on April 30th, and patched versions of Windows DNS Server are now available on their website (see Microsoft Security Bulletin MS07-062 and Microsoft Knowledge Base Article 941672).

Thanks,

Amit Klein  
CTO  
Trusteer

PS – as a side note, this vulnerability was originally scheduled for the October patch Tuesday, but due to some implementation issues, it was postponed by one month.