

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

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

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-05/msg00097.html>

---

- *From:* [rick.a.cook@xxxxxxxxxx](mailto:rick.a.cook@xxxxxxxxxx)
  - *Date:* 8 May 2008 14:37:31 -0000
- 

After implementing this patch on a large scale network, it was discovered that this patch caused a dns memory leak. Microsoft has since corrected this issue with a private fix. Even worse, in my large enterprise, this patch caused the exact spoofing that it intended to prevent. Somehow the code to increase the entropy has caused random xid's to cross and spoof randomly, poisoning the cache through normal usage without the use of extracurricular programs. I've reported this to Microsoft and have been working with them in fixing this issue, which to date has not been fixed.