

Re: [Full-disclosure] Microsoft DNS resolver: deliberately sabotagedhosts-file lookup

Re: [Full-disclosure] Microsoft DNS resolver: deliberately sabotagedhosts-file lookup

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-04/msg00466.html>

- *From:* "Thor (Hammer of God)" <thor@xxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 19 Apr 2006 19:59:40 -0700
-

You got a KB or some other official reference? I just did it again after a failed DNS lookup. Lookup failed, added it in the hosts file, worked just fine.

What exactly do you mean by "dns lookup failed?" The server is not available, or the host isn't found on the server? I just tested both ways – valid server with invalid host and invalid server. Ping resolution failed, added host, resolved immediately and attempted ping, removed it and saved, ping resolution immediately failed again; just like it is supposed to.

As I requested in my previous post, please provide us with detailed instructions on how to recreate this issue.

t

On 4/19/06 4:43 PM, "John Biederstedt" <john@xxxxxxxxxxxxxxxxx> spoketh to all:

Actually, according to microsoft, the dns client in XP was *intended* to check to see if a dns lookup had failed earlier before going to the hosts file.

We did ping the internal domain controller, added the bogus FQDN, and tried again. None of that worked, because prior to the VPN working, and lookup of the domain controller had failed, and been cached. So, because the failiure was checked before the hosts file, once the VPN was up, the dns lookups didn't work.

Oh yes, the XP install was factory Dell.