

DHCP security breach

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-06/msg00041.html>

- *From:* boomboom999@xxxxxxxxxx
 - *Date:* 14 Jun 2006 19:44:36 -0700
-

Hello,

I have an Active Directory integrated DNS zone configured for secure updates.

I am evaluating risks of permitting our DHCP server (Windows 2003-based one) to register A and PTR records on behalf of workstations (Windows XP).

If I understand correctly this option will compromise the whole idea of the Secure DNS updates.

As the DHCP protocol is not secured at all, DHCP has absolutely no means to validate who is requesting a DNS name update. So why Microsoft does not mention these risks of allowing DNS updates via DHCP servers. With a little effort, I can hijack any workstation's name.

Any ideas on how to secure DNS updates via DHCP?

.