Article ID: 968732 - Last Review: March 19, 2009 - Revision: 3.0

Changes to DNS server behavior after you install the security update for DNS server

INTRODUCTION

Post installation behavior on server computers after you install the DNS server security update

The purpose of this Knowledge Base article is to educate users about scenarios that are affected by an impending change to DNS server functionality. We have tried to make this document as generic as possible. Please read this document in its entirety and use it to understand if and how your enterprise environment may be affected by this update.

For more information about the DNS server security update, click the following article number to view the article in the Microsoft Knowledge Base:

961063 (http://support.microsoft.com/kb/961063/) MS09-008: Description of the security update for DNS server: March 10, 2009

MORE INFORMATION

Definitions table

Term	Definition
Domain Name System (DNS)	The Domain Name System is an Internet standard protocol that translates names to IP addresses and vice versa.
WPAD	Web Proxy Auto-discovery Protocol
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol

An overview of the security issue

Internet Explorer and similar clients search for a proxy server by using the Web Proxy Auto-discovery Protocol (WPAD). Client computers look for the WPAD server by resolving the name WPAD and by using DNS. ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is an IPv6 transition technology. DNS Clients perform ISATAP discovery, which is similar to the method that is used for WPAD. Malicious registration of a WPAD or ISATAP entry inside a corporate network could allow for an attacker to configure a malicious proxy. There are workarounds for the security problem. For example, you can register a reserved name host entry in the DNS database. The administrator must register the host name without registering an IP address, thereby reserving the name host entry.

Changes to DNS after you apply the security update

The following changes to DNS will occur after you apply the DNS security update:

- The security update automatically creates a block list that will be used by DNS. Every name query request is checked against the block list and a negative response is sent for the block listed name query.
- The block list default depends on the data in the zones that the server is authoritative for when the update is run. If the zone data does not contain entries for WPAD or ISATAP, then the WPAD or ISATAP entries are populated in the block list.
- If the DNS database already has any of these entries, then the WPAD or ISATAP entries are not populated in the block list.
- The administrator can configure and edit the block list in the registry. DNS service has to be restarted for accepting the new block list.
- For DNS, the block list applies to all zones that are hosted by the server. You cannot allow for WPAD and ISATAP queries in one zone but not another.
- The block list is stored in the registry for each server. There is no replication of block list entries across multiple servers.

Frequently asked questions

1. What happens if I upgrade my DNS server to LH server?
   Answer: A DNS server that uses valid entries of WPAD and ISATAP will continue to function as before.
2. What is the location of the registry entry for the block list?
   Answer: The block list uses the GlobalQueryBlockList REG_MULTI_SZ entry in the following subkey:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\GlobalQueryBlockList
3. What if I delete the entries of the block list in the registry?
   Answer: All queries to WPAD and ISATAP will succeed after a service restart if there is an entry for DNS at the time of service restart. If no WPAD entry is present at the start of the service, the default values are repopulated in the registry.
4. What if I add an entry "contoso" to the block list in the registry?
   Answer: After you add the entry in the block list, all queries to contoso in any zone will fail as soon as the service is restarted.
5. What happens if I already have an entry for contoso in the DNS database and I also add contoso in the

blocked list?
Answer: Queries to "contoso.*myzone*.com" will fail.

6. I have a WPAD server deployed in my network. Will I be affected?
   Answer: No. If you have WPAD deployed in a network, and you already have the name WPAD registered in DNS, then it will not be blocked. However, if you have WPAD in the network and it uses DHCP to distribute the wpad.dat file with nothing in DNS, then the DNS query for WPAD will be blocked.
7. Can I use DNSCMD.exe to configure the block list?
   Answer: No. You can only change the block list in the registry.
8. Would registration for blocked entries fail in the DNS server ?
   Answer: No. As part of the block list feature, registrations will succeed. Only queries for the blocked entries will fail.
9. Are only Host (type A or AAAA) queries blocked by this feature?
   Answer: No, all kinds of queries for the names in the block list are blocked.

APPLIES TO

- Microsoft Windows Server 2003 Service Pack 1, when used with:
  Microsoft Windows Server 2003, Standard Edition (32-bit x86)
  Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
  Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
  Microsoft Windows Server 2003, Web Edition
  Microsoft Windows Server 2003, Datacenter Edition for Itanium-Based Systems
  Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
- Microsoft Windows Server 2003, Datacenter x64 Edition
- Microsoft Windows Server 2003, Enterprise x64 Edition
- Microsoft Windows Server 2003, Standard x64 Edition
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 Service Pack 2, when used with:
  Microsoft Windows Server 2003, Standard Edition (32-bit x86)
  Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
  Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
  Microsoft Windows Server 2003, Web Edition
  Microsoft Windows Server 2003, Datacenter x64 Edition
  Microsoft Windows Server 2003, Enterprise x64 Edition
  Microsoft Windows Server 2003, Standard x64 Edition
  Microsoft Windows XP Professional x64 Edition
  Microsoft Windows Server 2003, Datacenter Edition for Itanium-Based Systems
  Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
- Microsoft Windows 2000 Service Pack 4, when used with:
  Microsoft Windows 2000 Advanced Server
  Microsoft Windows 2000 Datacenter Server
  Microsoft Windows 2000 Professional Edition
  Microsoft Windows 2000 Server

Keywords: kbexpertiseinter kbsecurity kbsecvulnerability kbsurveynew KB968732