DNS Server Global Query Block List

Microsoft Corporation

Published: November 2007

Author: Jim Groves

Editor: Jim Becker

Abstract

Clients of network protocols that rely on Domain Name System (DNS) name resolution to resolve well-known host names are vulnerable to malicious users who use dynamic update to register host computers that pose as legitimate servers. Examples of such protocols are the Web Proxy Auto-Discovery Protocol (WPAD) and the Intra-site Automatic Tunnel Addressing Protocol (ISATAP). The DNS server role in the Windows Server® 2008 operating system introduces a global query block list that can help reduce this vulnerability. This document introduces this block list, explains how it works, and describes how to take advantage of its features.

Microsoft

Contents

DNS server global query block list overview

Most TCP/IP networks support the dynamic update feature of Domain Name System (DNS) because dynamic update is convenient for network administrators and users alike. Dynamic update makes it possible for DNS client computers to register and dynamically update their resource records with a DNS server whenever a client changes its network address or host name. This reduces the need for manual administration of zone records, especially for clients that frequently move or change locations and use Dynamic Host Configuration Protocol (DHCP) to obtain an IP address. This convenience comes at a cost, however, because an authorized client can register any unused host name, even a host name that might have special significance for certain applications. This can allow a malicious user to "hijack" a special name and divert certain types of network traffic to that user's computer.

Two commonly deployed protocols are particularly vulnerable to hijacking in this fashion: the Web Proxy Automatic Discovery Protocol (WPAD) and the Intra-site Automatic Tunnel Addressing Protocol (ISATAP). Even if a network does not deploy these protocols, clients that are configured to use them are vulnerable to the hijacking that DNS dynamic update enables. To prevent such hijacking, the DNS server role in the Windows Server® 2008 operating system includes a global query block list that can help prevent a malicious user from hijacking DNS names that have special significance.

What is WPAD?

Most Web browsers use WPAD to locate and apply configuration settings that enable them to use a network proxy server. These configuration settings are contained in a file that is located on a server. The browser locates this server by querying a DHCP server for the uniform resource locator (URL) of the network's WPAD server. If this query is unsuccessful, the browser attempts to locate the WPAD server by using standard DNS name-resolution queries.

For example, if the Web browser is running on a Windows-based computer named laptop.acctg.corp.contoso.com, the browser attempts to find the WPAD configuration file by looking for the following URLs:

- http://wpad.acctg.corp.contoso.com/wpad.dat
- http://wpad.corp.contoso.com/wpad.dat
- http://wpad.contoso.com/wpad.dat

When it locates the Wpad.dat file at any of these locations, the browser reads the contents of the file, and then configures itself according to the settings in the file.

Unfortunately, you cannot secure this automatic discovery process. Any computer that is registered in a DNS zone with the name wpad can provide a WPAD configuration to clients on the network, even if the file contains settings that cause the clients to use a fake proxy server, for example, to divert the client's Web browser to counterfeit Web sites. The dynamic update feature of DNS makes it possible for a malicious user to accomplish this without requiring the intervention

of a DNS system administrator simply by giving a computer the name wpad and then connecting it to the network. As long as there is no other computer in the zone with the same name, the computer of the malicious user can register its name with the DNS server that is authoritative for its zone and thereby direct all WPAD queries to itself.

The block list feature that is provided by the DNS server role in Windows Server 2008 helps prevent the hijacking of WPAD by ensuring that queries for WPAD servers always fail unless WPAD is excluded from the block list. For more information about how the block list works, see How the DNS server block list works.

What is ISATAP?

ISATAP provides a transition between networks that are based on Internet Protocol version 4 (IPv4) and networks that are based solely on the newer IP version 6 (IPv6). ISATAP provides this transition by using a tunneling approach to carry IPv6 traffic on an IP version 4 (IPv4) infrastructure. In other words, ISATAP encapsulates IPv6 packets with an IPv4 header, which allows the IPv6 packets to be transmitted through a single ISATAP router from one ISATAP-enabled host to another. This transmission occurs wherever the hosts are located on the network, regardless of whether the hosts are located on an IPv6-enabled subnet or on an IPv4-only network.

ISATAP does not support automatic router discovery. Instead, ISATAP hosts use a potential routers list (PRL) to discover available ISATAP routers. Most commonly, however, ISATAP hosts construct their PRLs by using DNS to locate a host named isatap on the local domain. For example, if the local domain is corp.contoso.com, an ISATAP-enabled host queries DNS to obtain the IPv4 address of a host named isatap.corp.contoso.com.

Consequently, a malicious user can spoof an ISATAP router in much the same way as a malicious user can spoof a WPAD server: A malicious user can use dynamic update to register the user's own computer as a counterfeit ISATAP router and then divert traffic between ISATAP-enabled computers on the network. To prevent this, the Windows Server 2008 DNS Server service blocks name resolution of the isatap host name by default.

How the DNS server global query block list works

In its default configuration, the Windows Server 2008 DNS Server service maintains a list of names that, in effect, it ignores when it receives a query to resolve the name in any zone for which the server is authoritative. To accomplish this, the DNS Server service first checks queries against the list. Then, if the leftmost portion of the name matches an entry in the list, the DNS Server service replies to the query as though no resource record existed, even if there is a host (A) or host (AAAA) resource record in the zone for the name. In this way, if a host (A) or host (AAAA) resource record exists in the zone because a host has used dynamic update to register itself with a blocked name, the DNS Server service does not resolve the name.

The block list automatically applies to all zones for which the server is authoritative. For example, if the DNS server is authoritative for contoso.com and for europe.contoso.com, it ignores queries

for wpad.contoso.com as well as for wpad.europe.contoso.com. However, the DNS Server service does not ignore queries for names in zones for which it is not authoritative. Specifically, the DNS Server service does not ignore queries that it receives through a forwarder or a stub zone, or as a result of normal recursion or forwarding. If the block list causes the DNS Server service to ignore a request for a resource record that does exist in a zone, it logs an event that explains why it did so.

Important

All DNS servers that are authoritative for a zone must be running Windows Server 2008 and must be configured with the same block list to ensure consistent results when clients query for resolution of names in the block list.

Because the DNS Server service applies the block list for all resource records, not just host (A) or host (AAAA) resource records, it ignores queries for such resource record types as mail exchanger (MX) and service locator (SRV) resource records. However, because the DNS Server service does not apply the block list to zone names themselves, an administrator can create a zone named wpad.contoso.com, for example, and add host resource records to that zone. In this case, the DNS Server service continues to resolve host names in the wpad.contoso.com zone.

The initial contents of the block list depend on whether WPAD or ISATAP is already deployed when you add the DNS server role to an existing Windows Server 2008 deployment or upgrade an earlier version of Windows Server running the DNS Server service. The next section describes installation and upgrade scenarios and explains how the contents of the block list are affected.

Installation Scenarios for the DNS server role

The Domain Name System (DNS) server role global query block list helps protect your network's clients when you have not deployed the Web Proxy Auto-Discovery Protocol (WPAD) or the Intra-site Automatic Tunnel Addressing Protocol (ISATAP) on your network. If one of these protocols was deployed when you installed or upgraded the DNS Server service on a server running Windows Server 2008, the DNS Server service configures itself to exclude the deployed protocol from the block list. It does this to avoid interfering with the proper functioning of the protocol.

The following sections describe how the DNS Server service configures itself depending on whether one of the protocols in the default block list was deployed when you installed or upgraded the DNS Server service.

Installing the DNS server role when neither WPAD nor ISATAP is deployed

If neither WPAD nor ISATAP was deployed on the network when you installed or upgraded the DNS Server service on a server running Windows Server 2008, the DNS Server service configures the block list to ignore queries for hosts named wpad and isatap.

The DNS Server service configures the block list the first time that it runs after you install or upgrade it. Whenever the DNS Server service starts, it checks for the existence of a particular registry key. If that key does not exist, the DNS Server service has not yet configured the block list. The DNS Server service then enumerates all locally authoritative zones looking for existing host (A) or host (AAAA) resource records for the names wpad and isatap. When the DNS Server service fails to find these records, it stores the default list, which consists of entries for the names wpad and isatap, in the registry along with a registry key that indicates that the block list is enabled.

Configuration of the block list takes place only when the DNS Server service starts the first time after you install or upgrade it. If you subsequently implement WPAD or ISATAP on the network, you must configure the affected DNS servers to remove the corresponding name from their block lists. Similarly, if you subsequently remove WPAD or ISATAP from the network after you install the DNS Server role in Windows Server 2008, you must add the corresponding name to the block list of the affected DNS servers. For more information about configuring the DNS Server service, see Configuring the DNS server when you deploy or remove protocols.

Note

When the DNS Server service configures itself, it does not attempt to determine whether the existing resource record for a host named wpad or isatap identifies a legitimate deployed server. Before you upgrade a Windows-based DNS server to Windows Server 2008, ensure that the server's zones do not already contain resource records for these host names if the WPAD or ISATAP protocols are not deployed on the network.

Installing the DNS server role when WPAD or ISATAP is deployed

If WPAD or ISATAP is deployed on the network when the DNS Server service starts the first time after you install it, the DNS Server service configures the block list to avoid interfering with the deployed protocol. As described earlier in this section, the first time that the DNS Server service starts after you install or upgrade it, the DNS Server service enumerates the zones for which it is authoritative. If it finds a host (A or AAAA) resource record for a host named wpad or isatap, it removes the corresponding name from the block list before it stores the block list in the registry. This allows WPAD or ISATAP clients to locate the servers that support the respective protocol.

If you subsequently remove support for WPAD or ISATAP from your network, you should reconfigure the affected DNS servers to enable blocking resolution of the corresponding names. For more information, see Configuring the DNS server when you deploy or remove protocols.

Configuring the DNS server when you deploy or remove protocols

The Domain Name System (DNS) Server role configures the global query block list only when the DNS Server service first starts after you install or upgrade it. Configuration prevents the DNS Server service from improperly removing an item from the block list if you subsequently register a host named wpad or isatap in one of the server's zones.

If you deploy or remove the Web Proxy Auto-Discovery Protocol (WPAD) or the Intra-site Automatic Tunnel Addressing Protocol (ISATAP) after you deploy the DNS server role on a server running Windows Server 2008, you must update the block list. You update the block list on all DNS servers that host the zones that are affected by the change. The affected zones are those where you registered the WPAD or ISATAP servers.

For more information about updating the global block list, see DNS server global query block list technical reference.

Configuring the DNS server when you deploy WPAD or ISATAP

When you deploy WPAD or ISATAP, you must remove the corresponding name from the block list of all servers that are authoritative for the zone where you registered the WPAD or ISATAP server. To accomplish this, you run the **dnscmd /config /globalqueryblocklist** command to update the block list, which removes the corresponding name.

For example, if you deploy ISATAP in your network and register a router named isatap in a zone, you must run the following command on all DNS servers that are authoritative for that zone:

dnscmd /config /globalqueryblocklist wpad

This command replaces the existing block list with a list that consists of only the name wpad. This removes isatap from the default block list.

Note

Before you replace the block list, you should run the **dnscmd /info /globalqueryblocklist** command to verify the current contents of the block list.

Configuring the DNS server when you remove WPAD or ISATAP

When you remove WPAD or ISATAP from your network, you should configure the block list to prevent the hijacking that is described in DNS server global query block list overview. To do this, you add the appropriate name to the block list of the DNS servers that are authoritative for the zones where you previously registered the protocol's host name. To add the DNS server name to the block list, you run the **dnscmd /config /globalqueryblocklist** command.

For example, if you remove support for WPAD from your network, you should run the following command on all DNS servers that host the zone where the wpad name was registered:

dnscmd /config /globalqueryblocklist wpad isatap

This replaces the existing global query block list with a list that includes the name wpad.

Configuring the DNS server to block other names

The Domain Name System (DNS) Server role in Windows Server 2008 includes a global query block list. This block list mitigates security vulnerabilities that occur because the Web Proxy Auto-Discovery Protocol (WPAD) and the Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) employ both dynamic update and DNS name resolution. Although this is the primary purpose of the block list, you can add names to it to prevent resolution for host names other than wpad and isatap. For example, to prevent name resolution for a host named payroll in all the zones that a DNS server running Windows Server 2008 hosts, you can run the following command to add the name payroll to the default block list on the server:

dnscmd /config /globalqueryblocklist wpad isatap payroll

DNS server global query block list technical reference

This following sections provide technical details about how the global query block list is configured in the Domain Name System (DNS) Server service in Windows Server 2008.

Extensions to dnscmd

Windows Server 2008 extends the **dnscmd** command-line tool to make it possible for you to configure and control the global query block list. The following table shows the commands that you can use with **dnscmd**.

Command	Description
dnscmd /info /enableglobalqueryblocklist	Displays whether the global query block list is enabled. If the block list is enabled, this command returns the value 1. If the block list is not enabled, this command returns the value 0.
dnscmd /info /globalqueryblocklist	Displays the host names in the current block list, if any.

Command	Description
dnscmd /config /enableglobalqueryblocklist [**0** | **1**]	Enables or disables the block list. If you want the DNS Server service to ignore queries for the names in the block list, you set the value of this command to 1. If you want to disable the block list, you set the value of this command to 0. With a value of 0, the DNS Server service does not ignore queries for names in the block list.
dnscmd /config /globalqueryblocklist	Removes all names from the block list.
dnscmd /config /globalqueryblocklist *name* [*name*]…	Replaces the current block list with a list of the names that you specify. By default, the global query block list contains the following names: • isatap • wpad The DNS Server service can remove either or both of these names when the DNS Server service starts the first time. For more information, see Installation Scenarios for the DNS server role.

Global query block list registry values

The DNS Server service uses the following registry values to store configuration information for the block list:

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\EnableGlobaQueryBlockList**

  If you set the value of this registry key to 1 (the default), it instructs the DNS Server service to block name resolution in all zones that the server hosts for the names that are in the block list. If you set the value of this registry key to 0, it instructs the DNS Server service not to block name resolution for the names in the block list.

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\GlobalQueryBlockList**

  This registry key is a multistring value that contains the names that you want name resolution to block.