

---

# NAME SERVER VERIFIER

*Developed by Positive Technologies*

MOSCOW 2009



POSITIVE / TECHNOLOGIES®

# Introduction

---

Service name registration in local network allows attackers to hijack other users traffic and conduct “man-in-the-middle” attacks. An attacker who successfully conducted this attack could analyze target system Internet traffic including confidential data, such as passwords, credit card numbers, personal correspondence, etc.

There are several ways to register names in a network:

- 1) Registration on DNS or WINS name server;
- 2) Certain NetBIOS name usage in a network.

WPAD and ISATAP names are described in the document. These names are used in the following protocols, respectively:

- WPAD (Web Proxy Auto Discovery) is a method used by web clients to automatically locate a browser configuration file used to connect through proxy. The main reason that makes attacks via WPAD such dangerous is that it is widely used in default configuration. Attacks with WPAD protocols are described in a separate article (<http://www.securitylab.ru/analytics/379619.php>);
- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is an IPv6 transition mechanism meant to transmit IPv6 packets on top of an IPv4 network.

# 1 Vulnerabilities

In March 2009 Microsoft published updates for DNS and WINS servers which allow users to prevent a number of attacks with special names but (see the article <http://www.securitylab.ru/analytics/379619.php>) these updates do not eliminate all security problems in the network.

## 1.1 DNS server vulnerability in WPAD registration vulnerability

A man-in-the-middle attack vulnerability exists in DNS servers where dynamic update is used and ISATAP and WPAD are not already registered in DNS. This vulnerability could allow a remote authenticated attacker to spoof a web proxy thereby redirect Internet traffic to an address of the attacker's choice.

Vulnerable systems	Microsoft Windows 2000, Microsoft Windows Server 2003, Microsoft Windows Server 2008
Vulnerable component	DNS server
Maximum impact	«man-in-the-middle» attack
Available exploit	no
CVE identifier	CVE-2009-0093
Exploit vector	Local network
SecurityLab security level	Medium

## 1.2 WPAD WINS server registration vulnerability

A man-in-the-middle attack vulnerability exists in WINS servers. This vulnerability could allow a remote authenticated attacker to spoof a web proxy and thereby redirect Internet traffic to an address of the attacker's choice.

Potentially dangerous records could be registered on WINS server.

Vulnerable systems	Microsoft Windows 2000, Microsoft Windows Server 2003
Vulnerable component	WINS server
Maximum impact	«man-in-the-middle» attack
Available exploit	no
CVE identifier	CVE-2009-0094
Exploit vector	Local network
SecurityLab security level	Medium

## 2 Utility

Positive Technologies issued an utility to detect potentially dangerous entries in DNS and WINS services database. The utility also allows to scan available local network to detect hosts with this NetBIOS names.

System administrators and security administrators could control entries in name servers and hosts with dangerous NetBIOS names if they use the utility.



## 3 What checks are made and how to fix vulnerabilities

---

### 3.1 WINS server checks

---

1. Checks for potentially dangerous entries on WINS server (WPAD; WPAD.; ISATAP). If such entries are detected then check network devices with the names or install the update MS09-008.
2. Checks for possibility to register potentially dangerous entries on WINS server and further name resolving (WPAD; WPAD.; ISATAP).

If the vulnerability is detected then register static entries for potentially dangerous names or install the update MS09-008.

### 3.2 DNS server checks

---

Analyzing DNS zone name is required for the checks.

1. Checks for possibility to dynamically update DNS zone  
It is recommended to allow dynamic updates from authenticated hosts only. Disable zone dynamic updates if not necessary.
2. Checks for potentially dangerous entries in the DNS zone (wpad, isatap).  
If such entries are detected then check network devices with the names or install the update MS09-008.
3. Checks for possibility to register potentially dangerous entries in the DNS zone (wpad, isatap). Similar to WINS, a possibility of name resolving after registration is checked

If the vulnerability is detected then register static entries for potentially dangerous names or install the update MS09-008.

### 3.3 Checks for available sub network

---

The utility gets IP addresses of adapters installed on the host and then sends broadcast NetBIOS request to get IP addresses of computers with potentially dangerous NetBIOS names. Potentially dangerous NetBIOS names are WPAD, WPAD. and ISATAP.

It potentially dangerous name is detected it is necessary to analyze this host owner and take appropriate measures.

*Notes:*

- *The utility does not recognize DNS and WINS services so do not scan hosts without this services – it is useless;*
- *.NET Framework. Is required for the utility.*

## 4 About Positive Technologies

---

Positive Technologies [www.ptsecurity.com](http://www.ptsecurity.com) is among the key players in the IT security market in Russia.

The principal activities of the company include the development of integrated tools for information security monitoring (MaxPatrol); providing IT security consulting services and technical support; the development of the Securitylab [en.securitylab.ru](http://en.securitylab.ru) leading Russian information security portal.

Among the clients of Positive Technologies there are more than 40 state enterprises, more than 50 banks and financial organizations, 20 telecommunication companies, more than 40 plant facilities, as well as IT, service and retail companies from Russia, CIS countries, Baltic States, China, Ecuador, Germany, Great Britain, Holland, Iran, Israel, Japan, Mexico, South African Republic, Thailand, Turkey and USA.

Positive Technologies is a team of highly skilled developers, advisers and experts with years of vast hands-on experience. The company specialists possess professional titles and certificates; they are the members of various international societies and are actively involved in the IT security field development.



## 5 Links

---

1. Article by Sergey Rublev about WPAD technology weaknesses  
[http://www.securitylab.ru/download/articles/WPAD\\_weakness\\_en.pdf](http://www.securitylab.ru/download/articles/WPAD_weakness_en.pdf)
2. WPAD Registration Vulnerability (Microsoft Security Bulletin)  
<http://www.microsoft.com/technet/security/Bulletin/MS09-008.msp>
3. WPAD in Wikipedia  
[http://en.wikipedia.org/wiki/Web\\_Proxy\\_Autodiscovery\\_Protocol](http://en.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol)
4. DNS dynamic updates in Windows 2003 Server  
<http://support.microsoft.com/kb/816592>
5. Changes to WINS server behavior after you install the security update for WINS server  
<http://support.microsoft.com/kb/968731>
6. ISATAP in Wikipedia  
<http://en.wikipedia.org/wiki/ISATAP>