



CVE-2007-1692

Published on: 03/26/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:36 PM UTC

CVE-2007-1692

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Windows 2000](#) from [Microsoft](#) contain the following vulnerability:

The default configuration of Microsoft Windows uses the Web Proxy Autodiscovery Protocol (WPAD) without static WPAD entries, which might allow remote attackers to intercept web traffic by registering a proxy server using WINS or DNS, then responding to WPAD requests, as demonstrated using Internet Explorer. NOTE: it could be argued that

if an attacker already has control over WINS/DNS, then web traffic could already be intercepted by modifying WINS or DNS records, so this would not cross privilege boundaries and would not be a vulnerability. It has also been reported that DHCP is an alternate attack vector.

CVE-2007-1692 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
[text/html](#)

[XF win-wpad-information-disclosure\(33244\)](#)

SANS Internet Storm
Center; Cooperative
Network Security
Community - Internet
Security - isc

[isc.sans.org](https://isc.sans.org/text/html)
[text/html](#)

[MISC isc.sans.org/diary.html?storyid=2517](https://isc.sans.org/diary.html?storyid=2517)

Windows weakness can lead to network traffic hijacks - CNET News	web.archive.org text/html Inactive Link Not Archived	MISC news.com/Windows+weakness+can+lead+to+network+traffic+hijacks/2100-1002_3-6170229.html
How to configure Microsoft DNS and WINS to reserve WPAD registration	web.archive.org text/html Inactive Link Not Archived	MSKB 934864
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2007-1115
No Description Provided	web.archive.org text/html Inactive Link Not Archived	MLIST [ISN] 20070326 Windows weakness can lead to network traffic hijacks

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2003 Server	2000	All	small_business_server	All
Operating System	Microsoft	Windows 2003 Server	r2	All	datacenter_64-bit	All
Operating System	Microsoft	Windows 2003 Server	2000	All	small_business_server	All
Operating System	Microsoft	Windows 2003 Server	r2	All	datacenter_64-bit	All
cpe:2.3:o:microsoft:windows_2000:*****:						
cpe:2.3:o:microsoft:windows_2000:*****:						
cpe:2.3:o:microsoft:windows_2003_server:2000*:small_business_server:*****:						
cpe:2.3:o:microsoft:windows_2003_server:r2*:datacenter_64-bit:*****:						
cpe:2.3:o:microsoft:windows_2003_server:2000*:small_business_server:*****:						
cpe:2.3:o:microsoft:windows_2003_server:r2*:datacenter_64-bit:*****:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)