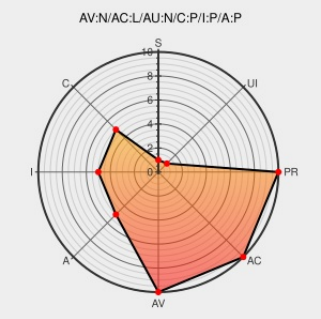
CVE-2007-1692

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 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 text/html	XF win-wpad-information-disclosure(33244)
SANS Internet Storm Center; Cooperative Network Security Community - Internet Security - isc	isc.sans.org text/html	MISC 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.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

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

← Previous ID

Next ID→