



CVE-2009-1930

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2009-1930
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-12 17:30:00 UTC
Updated	2023-12-07 18:38:00 UTC
Description	The Telnet service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Se

Risk And Classification

Problem Types: CWE-255

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2000	-	sp4	All	All
Operating System	Microsoft	Windows 2000	-	sp4	All	All
Operating System	Microsoft	Windows 2003 Server	sp2	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp2	All	itanium	All
Operating System	Microsoft	Windows 2003 Server	sp2	All	x64	All
Operating System	Microsoft	Windows 2003 Server	sp2	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp2	All	itanium	All
Operating System	Microsoft	Windows 2003 Server	sp2	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	-	x32	All
Operating System	Microsoft	Windows Server 2008	-	-	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	-	sp2	x86	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	-	x32	All

Operating System	Microsoft	Windows Server 2008	-	-	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	-	sp2	x86	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	-	-	x64	All
Operating System	Microsoft	Windows Vista	-	sp1	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	-	-	x64	All
Operating System	Microsoft	Windows Vista	-	sp1	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	x64	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All
Operating System	Microsoft	Windows Xp	All	sp2	x64	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All

References						
Reference						Source
Microsoft Windows Telnet NTLM Credential Reflection Authentication Bypass Vulnerability						BID
Microsoft Windows Telnet NTLM Credential Reflection Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com						SECUNIA
56904						OSVDB
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUPEN
SecurityTracker.com Archives - Microsoft Telnet NTLM Credential Reflection Flaw Lets Remote Users Gain Access						SECTRACKER
Repository / Oval Repository						OVAL
Microsoft Security Bulletin MS09-042 - Important Microsoft Docs						MS
US-CERT Technical Cyber Security Alert TA09-223A -- Microsoft Updates for Multiple Vulnerabilities						CERT
CVE Program record						CVE.ORG
NVD vulnerability detail						NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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