



CVE-2007-1205

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2007-1205
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-10 21:19:00 UTC
Updated	2018-10-16 16:37:00 UTC
Description	Unspecified vulnerability in Microsoft Agent (msagent\agentsvr.exe) in Windows 2000 SP4, XP SP2, and Server 2003, 2008

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2003 Server	gold	All	All	All
Operating System	Microsoft	Windows 2003 Server	gold	All	itanium	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	itanium	All
Operating System	Microsoft	Windows 2003 Server	sp1	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 2003 Server	gold	All	All	All
Operating System	Microsoft	Windows 2003 Server	gold	All	itanium	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	itanium	All
Operating System	Microsoft	Windows 2003 Server	sp1	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 Xp	All	gold	professional_x64	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	professional_x64	All
Operating System	Microsoft	Windows Xp	All	gold	professional_x64	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	professional_x64	All

References

Reference	Source	Link
US-CERT Technical Cyber Security Alert TA07-100A -- Microsoft Updates for Multiple Vulnerabilities	CERT	www.us-cert.gov
Microsoft Security Bulletin MS07-020 - Critical Microsoft Docs	MS	docs.microsoft.com
VU#728057 - Microsoft Windows Agent fails to properly process crafted URLs	CERT-VN	www.kb.cert.org
Microsoft Agent URL Parsing Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTrack	www.securitytracker.co
Microsoft Agent URL Parsing Memory Corruption Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Microsoft Agent URI Processing Remote Code Execution Vulnerability	BID	www.securityfocus.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
SecurityFocus	HP	www.securityfocus.com
SecurityFocus	BUGTRAQ	www.securityfocus.com
Microsoft Agent URL Parsing Memory Corruption Vulnerability - Secunia Research - Secunia	MISC	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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