



CVE-2009-0078

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

Summary

CVE	CVE-2009-0078
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-15 08:00:00 UTC
Updated	2023-12-07 18:38:00 UTC
Description	The Windows Management Instrumentation (WMI) provider in Microsoft Windows XP SP2 and SP3, Server 2003 SP1 and SP2, and Server 2008 SP2 and SP3 is vulnerable to a buffer overflow attack. An attacker could exploit this vulnerability to execute arbitrary code on the target system. The vulnerability exists in the WMI provider's handling of certain WQL queries. This vulnerability is present in the following versions of Windows: Windows XP SP2 and SP3, Windows Server 2003 SP1 and SP2, and Windows Server 2008 SP2 and SP3. Microsoft has released a security update to address this vulnerability. Users are advised to install the update as soon as possible.

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows Server 2003	All	All	All	All
Operating System	Microsoft	Windows Server 2003	All	sp1	All	All
Operating System	Microsoft	Windows Server 2003	All	sp1	itanium	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	All	All	All
Operating System	Microsoft	Windows Server 2003	All	sp1	All	All
Operating System	Microsoft	Windows Server 2003	All	sp1	itanium	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	All	All	All	All
Operating System	Microsoft	Windows Server 2008	All	All	32_bit	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	All	All	All
Operating System	Microsoft	Windows Server 2008	All	All	32_bit	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Vista	All	All	All	All

Operating System	Microsoft	Windows Vista	All	All	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	gold	All	All	All
Operating System	Microsoft	Windows Vista	All	All	All	All
Operating System	Microsoft	Windows Vista	All	All	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	gold	All	All	All
Operating System	Microsoft	Windows Xp	All	All	pro_x64	All
Operating System	Microsoft	Windows Xp	All	sp1	All	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	pro_x64	All
Operating System	Microsoft	Windows Xp	All	All	pro_x64	All
Operating System	Microsoft	Windows Xp	All	sp1	All	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	pro_x64	All

References	
Reference	Source
53666	OSVDB
Microsoft Windows Privilege Separation and Access Control Bugs Let Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK
US-CERT Technical Cyber Security Alert TA09-104A -- Microsoft Updates for Multiple Vulnerabilities	CERT
Microsoft Security Bulletin MS09-012 - Important Microsoft Docs	MS
Repository / Oval Repository	OVAL
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
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.

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