



# CVE-2008-3009

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2008-3009
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@microsoft.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-12-10 14:00:00 UTC
<b>Updated</b>	2023-12-07 18:38:00 UTC
<b>Description</b>	Microsoft Windows Media Player 6.4, Windows Media Format Runtime 7.1 through 11, and Windows Media Services 4.1, 9

## 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	All	sp4	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Application	Microsoft	Windows Media Format Runtime	11	All	All	All
Application	Microsoft	Windows Media Format Runtime	11	All	x64	All
Application	Microsoft	Windows Media Format Runtime	7.1	All	All	All
Application	Microsoft	Windows Media Format Runtime	9	All	All	All
Application	Microsoft	Windows Media Format Runtime	9.5	All	All	All
Application	Microsoft	Windows Media Format Runtime	9.5	All	x64	All
Application	Microsoft	Windows Media Format Runtime	11	All	All	All
Application	Microsoft	Windows Media Format Runtime	11	All	x64	All
Application	Microsoft	Windows Media Format Runtime	7.1	All	All	All
Application	Microsoft	Windows Media Format Runtime	9	All	All	All
Application	Microsoft	Windows Media Format Runtime	9.5	All	All	All
Application	Microsoft	Windows Media Format Runtime	9.5	All	x64	All
Application	Microsoft	Windows Media Player	6.4	All	All	All
Application	Microsoft	Windows Media Player	6.4	All	All	All
Application	Microsoft	Windows Media Services	2008	All	All	All

Application	Microsoft	Windows Media Services	4.1	All	All	All
Application	Microsoft	Windows Media Services	9	All	All	All
Application	Microsoft	Windows Media Services	2008	All	All	All
Application	Microsoft	Windows Media Services	4.1	All	All	All
Application	Microsoft	Windows Media Services	9	All	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	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	sp2	All	All
Operating System	Microsoft	Windows Server 2008	All	All	x32	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	All	x32	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	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	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	All	x64	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	sp3	All	All
Operating System	Microsoft	Windows Xp	All	All	pro_x64	All
Operating System	Microsoft	Windows Xp	All	All	x64	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	sp3	All	All

## References

## Reference

Windows Media Player Service Principal Name NTLM Authentication Implementation Lets Remote Users Execute Arbitrary Code - SecurityTr

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Microsoft Windows Media Components 'Service Principle Name' Remote Code Execution Vulnerability

Microsoft Windows Media Products Two Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Microsoft Security Bulletin MS08-076 - Important | Microsoft Docs

Windows Media Services Service Principal Name NTLM Authentication Implementation Lets Remote Users Execute Arbitrary Code - Security

Repository / Oval Repository

US-CERT Technical Cyber Security Alert TA08-344A -- Microsoft Updates for Multiple Vulnerabilities

CVE Program record

NVD vulnerability detail



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](#).

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