



CVE-2009-1544

Published on: 08/12/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:26 PM UTC

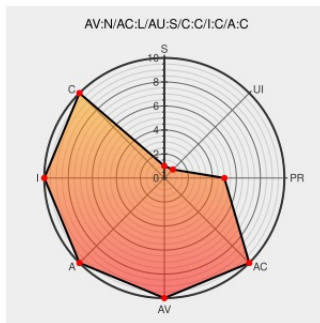
CVE-2009-1544

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Windows 2003 Server](#) from [Microsoft](#) contain the following vulnerability:

Double free vulnerability in the Workstation service in Microsoft Windows allows remote authenticated users to gain privileges via a crafted RPC message to a Windows XP SP2 or SP3 or Server 2003 SP2 system, or cause a denial of service via a crafted RPC message to a Vista Gold, SP1, or SP2 or Server 2008 Gold or SP2 system, aka "Workstation Service Memory Corruption Vulnerability."

CVE-2009-1544 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Microsoft Security Bulletin MS09-041 - Important Microsoft Docs	docs.microsoft.com text/html	MS MS09-041
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval.org/mitre.oval:def:6286
US-CERT Technical Cyber Security Alert TA09-223A -- Microsoft Updates for Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/xml	CERT TA09-223A

By selecting these links, you may be leaving CVEreport workspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [CVEreport](#).

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 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	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All

Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	-	-	x64	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 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
cpe:2.3:o:microsoft:windows_2003_server:sp2:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:sp2:*:itanium:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:sp2:*:x64:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:sp2:*:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:sp2:*:itanium:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:sp2:*:x64:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:*:*:itanium:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008*:sp2:x64:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:-:x32:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:-:x64:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:itanium:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:x86:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:*:*:itanium:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008*:sp2:x64:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:-:x32:*:*:*:*:						

cpe:2.3:o:microsoft:windows_server_2008:-:-:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:itanium:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:x86:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp2:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:-:-:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp2:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:-:-:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:sp2:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:-:-:sp2:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:-:sp3:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:sp2:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:-:-:sp2:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:-:-:sp3:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)