



Published on: 10/11/2005 12:00:00 AM UTC

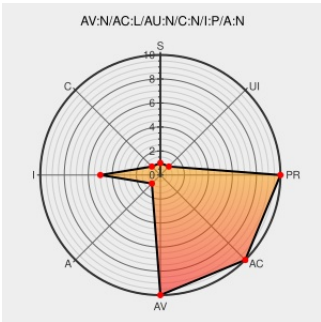
Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2119

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Windows 2000](#) from [Microsoft](#) contain the following vulnerability:

The `MIDL_user_allocate` function in the Microsoft Distributed Transaction Coordinator (MSDTC) proxy (`MSDTCPRX.DLL`) allocates a 4K page of memory regardless of the required size, which allows attackers to overwrite arbitrary memory locations using an incorrect size value that is provided to the `NdrAllocate` function, which writes memory outside of the allocated buffer.

CVE-2005-2119 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Microsoft Windows MSDTC Memory Corruption Vulnerability	cve.report (archive) text/html	 BID 15056
SecurityReason	securityreason.com text/html	 SREASON 73
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:1452
Network Security, Vulnerability Assessment, Intrusion Prevention	www.eeye.com text/html	 EYE AD20051011b
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:1071

SecurityTracker.com Archives - Microsoft Windows Buffer Overflows in MSDTC and COM+ Let Remote Users Execute Arbitrary Code and Local User Gain Elevated Privileges	securitytracker.com text/html	 SECTrack 1015037
Secunia - Advisories - Microsoft Windows MSDTC and COM+ Vulnerabilities	web.archive.org text/html	 SECUNIA 17161
Secunia - Advisories - Avaya Various Products Multiple Vulnerabilities	web.archive.org text/html	 SECUNIA 17172
Secunia - Advisories - Nortel CallPilot Multiple Vulnerabilities	web.archive.org text/html	 SECUNIA 17509
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:551
	support.avaya.com application/pdf	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2005-214.pdf
US-CERT Vulnerability Note VU#180868	US Government Resource www.kb.cert.org text/html	 CERT-VN VU#180868
Secunia - Advisories - Nortel Centrex IP Client Manager Multiple Vulnerabilities	web.archive.org text/html	 SECUNIA 17223
US-CERT Technical Cyber Security Alert TA05-284A -- Microsoft Windows, Internet Explorer, and Exchange Server Vulnerabilities	US Government Resource www.us-cert.gov text/html	 CERT TA05-284A
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 18828
Microsoft Security Bulletin MS05-051 - Critical Microsoft Docs	docs.microsoft.com text/html	 MS MS05-051

By selecting these links, you may be leaving CVEreport webspace. 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 comment@cve.report.

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 2000	All	sp4	All	fr
Operating System	Microsoft	Windows 2000	All	sp4	All	fr
Operating System	Microsoft	Windows 2003 Server	64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	itanium	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	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	64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	itanium	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	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 Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	sp1	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	sp1	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All
cpe:2.3:o:microsoft:windows_2000:*:sp4:*:fr:*:*:*:						
cpe:2.3:o:microsoft:windows_2000:*:sp4:*:fr:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:64-bit:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:itanium:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:r2:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:sp1:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:sp1:*:itanium:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:64-bit:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:itanium:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:r2:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:sp1:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:sp1:*:itanium:*:*:*:*:						

cpe:2.3:o:microsoft:windows_xp:*:*:64-bit:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:sp1:tablet_pc:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:sp2:tablet_pc:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:*:64-bit:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:sp1:tablet_pc:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:sp2:tablet_pc:*:*:*:*:

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](#)