



# CVE-2007-1765

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

## Summary

<b>CVE</b>	CVE-2007-1765
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-03-30 00:19:00 UTC
<b>Updated</b>	2021-07-23 12:16:00 UTC
<b>Description</b>	Unspecified vulnerability in Microsoft Windows 2000 SP4 through Vista allows remote attackers to execute arbitrary code or

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Avaya</a>	<a href="#">Definity One Media Server</a>	All	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">Definity One Media Server</a>	All	All	All	All
Application	<a href="#">Avaya</a>	<a href="#">Ip600 Media Servers</a>	All	All	All	All
Application	<a href="#">Avaya</a>	<a href="#">Ip600 Media Servers</a>	All	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S3400</a>	All	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S3400</a>	All	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8100</a>	All	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8100</a>	All	All	All	All
Application	<a href="#">Microsoft</a>	<a href="#">Ie</a>	7.0	All	vista	All
Application	<a href="#">Microsoft</a>	<a href="#">Ie</a>	7.0	All	vista	All
Application	<a href="#">Microsoft</a>	<a href="#">Ie</a>	All	All	All	All
Application	<a href="#">Microsoft</a>	<a href="#">Internet Explorer</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 2000</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 2000</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 2000</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 2000</a>	All	All	All	ja
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 2000</a>	All	sp1	All	All





Reference	Source	Link
McAfee Threat Center – Latest Cyberthreats   McAfee	MISC	<a href="#">www.a</a>
Microsoft Windows Cursor And Icon ANI Format Handling Remote Buffer Overflow Vulnerability	BID	<a href="#">www.s</a>
SecurityTracker.com Archives - Microsoft Windows Animated Cursor Bug Lets Remote Users Execute Arbitrary Code	SECTRACK	<a href="#">www.s</a>
Resources   BeyondTrust	MISC	<a href="#">resear</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.v</a>
SecurityFocus	BUGTRAQ	<a href="#">www.s</a>
SecurityFocus	BUGTRAQ	<a href="#">www.s</a>
Your request has been blocked. This could be due to several reasons.	CONFIRM	<a href="#">www.n</a>
<a href="#">vil.nai.com/vil/content/v_141860.htm</a>	MISC	<a href="#">vil.nai.</a>
McAfee Threat Center – Latest Cyberthreats   McAfee	MISC	<a href="#">www.a</a>
Any ANI File Could Infect You! · Security to the Core   Arbor Networks Security Blog	MISC	<a href="#">asert.a</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis</a>

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](#)**