



CVE-2006-6696

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

Summary

CVE	CVE-2006-6696
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-12-22 02:28:00 UTC
Updated	2019-04-30 14:27:00 UTC
Description	Double free vulnerability in Microsoft Windows 2000, XP, 2003, and Vista allows local users to gain privileges by calling the

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	All	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	enterprise	All
Operating System	Microsoft	Windows 2003 Server	standard	All	All	All

Operating System	Microsoft	Windows 2003 Server	standard	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	All	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	enterprise	All
Operating System	Microsoft	Windows 2003 Server	standard	All	All	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1_beta_1	All	All
Operating System	Microsoft	Windows Vista	All	All	december_ctp	All
Operating System	Microsoft	Windows Vista	All	beta	All	All
Operating System	Microsoft	Windows Vista	All	beta1	All	All
Operating System	Microsoft	Windows Vista	All	beta2	All	All
Operating System	Microsoft	Windows Vista	All	All	december_ctp	All
Operating System	Microsoft	Windows Vista	All	beta	All	All
Operating System	Microsoft	Windows Vista	All	beta1	All	All
Operating System	Microsoft	Windows Vista	All	beta2	All	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	media_center	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	home	All
Operating System	Microsoft	Windows Xp	All	sp2	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	media_center	All

Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	home	All
Operating System	Microsoft	Windows Xp	All	sp2	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All

References						
Reference				Source	Link	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vupen.com	
Welcome to the Microsoft Security Response Center Blog! : New report of a Windows vulnerability				CONFIRM	blogs.technet.com	
[Full-disclosure] Microsoft Windows XP/2003/Vista memory corruption 0day				FULLDISC	lists.grok.org.uk	
Microsoft Windows CSRSS Privilege Escalation Vulnerability - Advisories - Secunia				SECUNIA	secunia.com	
eEye Digital Security - Research				MISC	research.eeye.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vupen.com	
Microsoft Windows memory corruption				MISC	www.security.nno	
Google Groups				MISC	groups.google.ca	
Repository / Oval Repository				OVAL	oval.cisecurity.org	
Windows CSRSS HardError Message Box Vulnerability				MISC	www.determina.com	
Microsoft Windows CSRSS MSGBox Remote Code Execution Vulnerability				BID	www.securityfocus.com	
SecurityFocus				BUGTRAQ	www.securityfocus.com	
SANS Internet Storm Center; Cooperative Network Security Community - Internet Security - isc				MISC	isc.sans.org	
SecurityFocus				HP	www.securityfocus.com	
SecurityFocus				BUGTRAQ	www.securityfocus.com	
3proxy tiny free proxy server for Windows, Linux, Unix: SOCKS, HTTP, FTP proxy				MISC	www.security.nno	
Microsoft Windows CSRSS HardError Messages Denial of Service Vulnerability				BID	www.securityfocus.com	
Microsoft Security Bulletin MS07-021 - Critical Microsoft Docs				MS	docs.microsoft.com	
SecurityFocus				BUGTRAQ	www.securityfocus.com	
404 Not Found				MISC	www.kuban.ru	
SecurityFocus				BUGTRAQ	www.securityfocus.com	
Windows Client-Server Run-time Subsystem Lets Remote Users Execute Arbitrary Code - SecurityTracker				SECTRAK	securitytracker.com	
SecurityFocus				BUGTRAQ	www.securityfocus.com	
CVE Program record				CVE.ORG	www.cve.org	
NVD vulnerability detail				NVD	nvd.nist.gov	

No vendor comments have been submitted for this CVE.

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](#).

Free CVE JSON API [cve.report/api](#)

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